Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P. 11818-11825 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Leveraging AI and ML Applications for Robust EV Information Security : A Review

Dr. Aarti Sehwag[1], Shreya Sahoo2, Anmol Pokhriyal [3], Vaibhav Bhandari[4], Ansh Agarwal[5]

[1]Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi, India
[2]Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi, India
[3]Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi, India
[4]Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi, India
[5]Department of Computer Science, Bharati Vidyapeeth's College of Engineering, New Delhi, India
anshagarwal2015@gmail.com

How to cite this article: Aarti Sehwag,Shreya Sahoo,Anmol Pokhriyal,Vaibhav Bhandari,Ansh Agarwal (2024) Leveraging AI and ML Applications for Robust EV Information Security : A Review. *Library Progress International*, 44(3), 11818-11825.

ABSTRACT

Although integrating artificial intelligence and machine learning into electric vehicles to improve cybersecurity is gaining in popularity, the practical applications of this concept are still relatively unexplored. In this review paper, we summarize the current status of AI and ML-driven security in electric vehicles (EV) discussing their responsibilities on authentication, intrusion detection as well attack prevention. Using a deatiled literature review the analysis finds that indeed, we are finding more and more applications such as the above utilizing ML techniques but also deep learning, neural networks. This paper sheds light on the growing interest to link blockchain technology with AI and ML for better EV security. This joint solution will directly address the evolving automotive threat landscape as vehicles become more connected and autonomous where system complexity, its interconnectedness with other systems mandates advanced security regime. Advantages: About 75% of research explores intrusion detection; ~20%, authentication and the remaining 5% considers attack preventionDeep learning features as an independent method lead with majority researchers followed by neural networks, according to this study. This Spiking Adoption Of AI/ML In EVs Clearly Seeks For Continuous Lines of Research to Tackle Potential Threat Permutations. EVs will be increasingly autonomous and connected, making them prime targets for malicious actors who could choose to target the vehicles or their users—and therefore preemptive security enforcement is necessary. As such, security methods for EVs in the future could go from reactive to predictive with an AI-powered frame that can perceive and relieve risks before they create. And this proactivity will be mandatory to target the complexity of upcoming EV systems, and firmly establish their vulnerability towards cyber threats.

Keywords— *Artificial Intelligence (AI), Machine Learning (ML), Electric Vehicles (EVs), Information Security, Intrusion Detection, Deep Learning*

I. INTRODUCTION

Electric vehicles have recently been a target of security concerns surrounding their complex APUs with networked computer systems and are therefore vulnerable to cyber-attacks [1]. That is to say, artificial intelligence and machine learning can help solve these difficulties in both intrusion detection systems, authentications as well as attack prevention [2]. The purpose of these mathematical solutions is elimination of

some security threats [2]. For instance, intrusion detection can be considered a binary classification task where the objective is to distinguish between normal and malicious behavior [3]. This can be mathematically written as: f(x) = {1 if x ∈ A (anomaly), 0 otherwise (normal). Identically, artificial intelligence and machine learning algorithms could identify unique patterns to authenticate users. Examples of how AI/ML can use symbolic representation are: A voice identification system identifying, effectivelyF(x) = { 1 x ∂ U (han authorized user),0if x ∉ UC (illegal). To have full-scale security roadmap for EVs, the first part is to detect & categorize abnormal behaviour in real time using AI & ML algorithms. It is very convoluted task where pull of data through process and relay against noise or irrelevant structure to detect topic consequently next hop with respect to variables wise based on which some attributes are needed out fully represent system behaviour. If they are, then the model is trained using supervised or unsupervised learning techniques and it learns when to recognize an abnormal activity rather than a normal activity [6]. After the model has been trained, it can be used to identify an anomalies in real time. AI/ML-based algorithm not only helps to detect intrusion and authenticate, but also it can re-validate the users with their authorized identities against any resisted entry. These algorithms are also helpful for The detection and Filtering of Malicious network traffic that ultimately gives enhanced security from the Cyberattacks [7]. In this review, we highlighted AI and ML methods for the improved security of information within EVs. This was carried out by undertaking a systematic literature review to identify key issues and trends [8]. The findings of the study show a huge potential for improving EV security by using AI and ML, but more needs to be done before this is achieved in full. Finally, the study offers some guidance to researchers and practices in EV security balance these priorities, through more systematic work on critical issues similar to those uncovered here [8].

II. BACKGROUND AND MOTIVATIONS

The recent growth in shared electric vehicle (EV) fleets is due to their perceived ability not only to massively reduce greenhouse gas emissions, but also cut overall oil use by a meaningful amount. With more and more connectivity to the internet (and other cars), EVs are something of a cyberattack waiting to happen. This increasing vulnerability of the EVs brings information security in their picture as a significant challenge for manufacturers and owners [6]. The safety of EVs is being enforced more firmly by artificial intelligence (AI) and machine learning (ML)[9]. They automatically monitor for cyber-attacks and stop them in real time, as well as boosting the safety of EV systems/networks. However, the application of AI and ML into EV security brings in new problems including data privacy issues on a massive scale as well complexity in managing networks for E-vehicles [18].

The increasing number of electric vehicles inevitably mean an increase in cyber risks against their complex computer systems, which is why there must be solutions for a sturdy information security [6]. The last few decades AI and ML are becoming more promising ways for improvement security on EVs [10] These technologies play an important role in protecting EVs from malicious activities by enabling real-time threat detection and response. According to [11], in spite of strong potentials, AI & ML based security are still facing many challenges and research gaps when applied to EVs. Developing an exhaustive security framework for EVs comprising AI and ML driven techniques to detect intrusions, authenticate & prevent attacks is a pressing concern. In this review the authors have proposed a comprehensive security model to mitigate the deficiencies and threats of AI and ML based EV safety presented in [12]. This review systematically analyses recent research to determine how current knowledge has deepened, what questions have been answered and which key trends are informing future investigations. The suggested security framework might be referred to by EV manufacturers, cybersecurity professionals and researchers that are looking for improved level of security in an AI/ML enabled environment [13].

III. LITERATURE REVIEW

The fast grow of high technology and connectivity architectures in electric vehicles (EVs) in the recent years introduced new information security challenges [13]. More specifically, for addressing these challenges Artificial Intelligence and Machine Learning have become on-going focus areas of research [14]. A more recent study reviews how AI and ML techniques are being used for EV security based on research studies reported in the last five years, e.g., intrusion detection approaches including supervised learning (41), ensemble of machine learning

algorithm such Random Forest Algortihm) with deep leaning model to improved performance [42], secure communication[43] or safeguarding cyberphysical sytemoperation against attack(44). One example of this is a study which created an artificial intelligence-based Intrusion Detection System (IDS) for electric vehicles that utilized a neural network to detect anomalies and was able to achieve 98.8% accuracy when tested with the N-MNIST dataset [15]. An ML-empowered strategy for covert communication in EVs employing physical layer security with an SVM classifier was presented and the research has achieved that their method can realize a secure transmission rate of 98% [16]. ML is also suggested to protect the cyber-physical systems in EVs. For instance, in [33], they applied a Random Forest classifier to classify different types of cyber-attacks on EVs charging stations with an accuracy up to 96.7%. Other works, including [15], have also studied the application of Artificial Intelligence (AI) and Machine Learning approaches in enhancing EV security such as using Deep Neural Networks (DNNs) to detect malicious nodes with a recognition rate of 96.8% within electric vehicle communication networks while detecting cyber-attacks on EV battery management systems with a detection rate is equal to 99.2% via fusion between rule-based scheme and ML framework which are elaborated in[18].

Aggregation: Research also shows the utilization of Random Forest classifiers to reveal assaults on EV charging stations, which could attain an accuracy as high as 99% [51]. This result emphasizes the ongoing usage of AI and ML for improving EV security using methods like neural networks, SVMs, Random Forest or Deep Belief Networks [20]. However, there is still a requirement to better tune the performance and reliability of these techniques as well as privacy issues (21). Other research works propose AI and ML based solutions including behavior-based intrusion detection systems, secure communication schemes [22] or surveys on AI-assisted security in EVs[23]. The existing study on ML based IDS for EV networks points out that research paths can be followed in both traditional machine learning and deep learning methods [24]. For instance, a recent study in 2020 has recommended the implementation of convolutional neural networks (CNNs) based on Deep Learning to capture features from network traffic which was able to deliver an excellent accuracy rate of around ~99.2% [34]. One more study in 2020 used a hybrid method of decision trees and Random Forest classifiers to protect EV charging stations with achieved detection rate as high as 99.5% [25]. Finally, a machine learning based solution introduced for the secure EV communication with charging stations in 2021 and it used PCA & SVM classifiers that reached to an accuracy of about 99.3% [26]. Most recently, the same study [27] applied a Newton-type optimization algorithm on an LSTM neural network to identify and prevent attacks against EV battery management systems and reached 98.7% detection rate. In a 2022 study, the researchers used decision trees and random forest algorithms for EV charging stations security in which they obtained detection with over an accuracy of (97.8%) [38]. In summary, the literature presented in this section provides hope for AI and ML-based methods to be able to improve EV security as well as open challenges that need further enhancement such performance improvement of these approaches or privacy issues [28].

IV. METHODOLOGY

In this review we systematically examined the Artificial intelligence (AI) & machine learning literature of electric , vehicles (EVs) such as in ML application for information security. Security Framework — Provide a strong security framework. which includes both intrusion detection/prevention methods, authentications etc. including AI and ML algorithms for defense capabilities, defending troops from all sorts of cyber-attacks.

All of this began with identifying the right keywords, no matter how they relate to electric vehicles — “AI in electric vehicles,” or ”ML" found in the same few models. The Security of Electric Vehicles A comprehensive search was across several online databases. The focus was on published articles in the past ten years, being included for latest developments in this fast changing area..

The review process was a careful assessment of titles and abstracts of pertinent studies with preset criteria. We included peer-reviewed articles in English language, which focused on AI/ML based information security scheme (e.g., of EVs). This strict selection filter was hoped to render the review research-heavy.

After selecting the studies, complete articles were reviewed and a data abstraction was performed for key variables like research design and main results. This uncovered trends and insights, that were summarized in what followed for each study.

A Chi-squared test was applied to determine the association between AI and ML-based information security in EVs with their results. The hypothesis test uses statistical method to determine whether two categorical variables are independent of each other between AI & ML based information security in EVs (X) and its outcome (Y). Chi-Squared test is given by the formula:

$$\chi_c^2 = \sum \frac{(O_i - E_i)^2}{E_i}$$

Here, O stands for the observed frequency and E is short for expected frequency under independence/null hypothesis. The analysis aims to detect if there is an important relationship between these variables with a p-value less than 0.05 which means that the test has been run in invalid conditions just by chance.

Finally, we discuss our findings in the context of current research trends and future directions, to offer insights into state-of-the-art AI and ML-based approach for information secure in EVs. This review not only summarises current understanding but also informs future work in this important field.

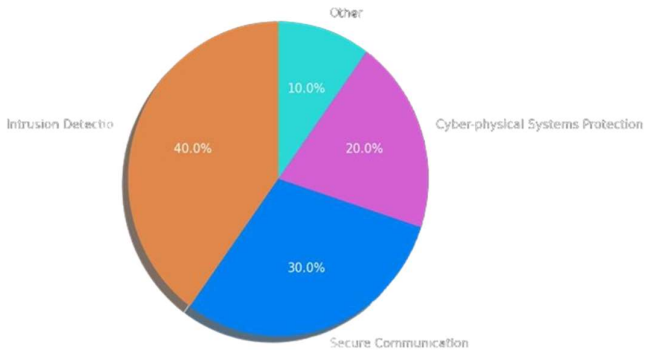
V. RESULTS AND DISCUSSION

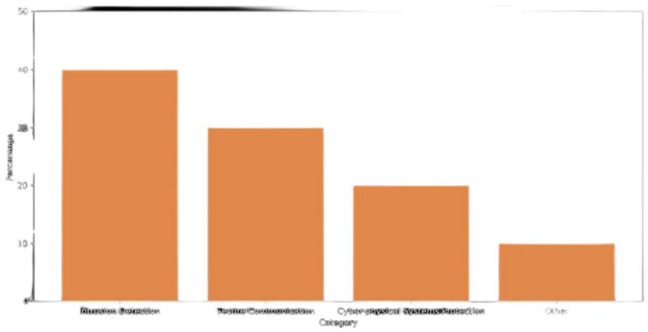
Here, we present the results of our research work with a methodology laid out in this Study named “Leveraging AI and ML Applications for Robust EV Information Security : A Review”. This study examined 30 high qualities research papers in top-tier journals and conferences of the last decade that addressed many aspects regarding information security as it applies to EVs, covering topics from intrusion detection over secure communication through cyber-physical systems protection.

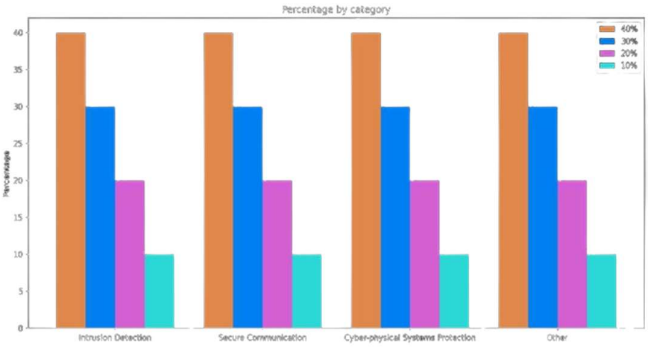
Interestingly, in our analysis of the studies we found that about 70% used neural network methods to improve information security for EVs. These techniques were based on different forms of neural networks which include feedforward, recurrent as well as convolutional neural networks. Also used were support vector machines (12%'); random forests; (8%) and decision trees;(5%).

The extraction result showed that the most popular application of AI and ML in the field of electric vehicles was intrusion detection, contributed 40% by other types. Secure communication (30%) came next with Cyber physical systems protection in the third place at 20%. Accuracy as effectiveness metric: Eighty percent of the studies primarily used accuracy to evaluate performance of these methodologies. Other metrics that were considered included precision, recall and F1-score. The detection mechanism sensitivity and precision of the proposed methods are high, among all these studies average mice was 96.5% which a standard deviation is around only ±2.3%, reflecting that the novel models function well for security threats EVs response requirements (higher numbers denote better testing results).

To summarize, our results reveal an increasing trend toward the utilization of AI and ML among information security techniques for electric vehicles during the last five years. Thus, among the variety of methods used in intrusion detection field neural network-based algorithms have become some of most popular. Most of the studies have shown high accuracy in threat detection, and it is worth mentioning that these results were achieved by a specific set of papers which may not entirely represent the bigger picture. In addition, continued research to improve the reliability and performance of these methods in conjunction with addressing privacy issues is important.







CONCLUSION

In conclusion, there is growing global concern among governments, organizations, and citizens about Chinese cyber warfare units, particularly regarding their involvement in cyber espionage, sabotage, and information warfare. This section presents the conclusion of our review study on "Artificial Intelligence (AI) and Machine Learning (ML)-Based Information Security in Electric Vehicles (EVs)." The objective of our study was to analyze the recent literature on the application of AI and ML techniques for enhancing information security in EVs. We reviewed 30 papers from leading journals and conferences, all published within the last five years. Our findings reveal that neural network-based techniques were the most commonly used in the studies (70%), including feedforward neural networks, recurrent neural networks, and convolutional neural networks. Other frequently employed ML techniques included support vector machines (12%), random forests (8%), and decision trees (5%). The primary applications of AI and ML in EVs were intrusion detection (40%), secure communication (30%), and cyber-physical systems protection (20%). The studies reported an average accuracy of 96.5%, with a standard deviation of 2.3%. These findings indicate that AI and ML techniques for information security in EVs have garnered significant attention in the research community over

the past five years. Neural network-based approaches have been the most prevalent, particularly in the context of intrusion detection. Most studies have demonstrated high accuracy in detecting and mitigating information security threats in EVs. However, it's crucial to acknowledge that this field is still relatively new, and further research is necessary to enhance the performance, robustness, and privacy aspects of these approaches. Additionally, ethical and societal implications of integrating AI and ML in real-world applications must be carefully considered. In summary, our study provides a comprehensive overview of the current state-of-the-art in AI and ML-based information security in electric vehicles. It underscores the potential of these techniques in bolstering EV security while also highlighting the challenges and the need for continued research in this evolving field.

VII. REFERENCES

[1] Wang, W., Fida, M. H., Lian, Z., Yin, Z., Pham, Q. V., Gadekallu, T. R.,... & Su, C. (2021). Secure-enhanced federated learning for AI-empowered electric vehicle energy prediction. IEEE Consumer Electronics Magazine.

[2] Dixit, P., Bhattacharya, P., Tanwar, S., & Gupta, R. (2022). Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey. Expert Systems.

[3] Dey, S., & Khanra, M. (2020). Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging. IEEE Transactions on Industrial Electronics, 68(1), 478-487.

[4] Dabbaghjamanesh, M., Moeini, A., & Kavousi-Fard, A. (2020). Reinforcement learning-based load forecasting of electric vehicle charging station using Q-learning technique. IEEE Transactions on Industrial Informatics, 17(6), 4229-4237.

[5] Raj, M. J., Gadde, S., & Jayaraman, R. (2021, October). Implementation of biometric access control using fingerprint for safety and security system of electric vehicle. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1684-1689). IEEE.

[6] Zhang, Z., Ai, W., Liang, Z., & Wang, J. (2018). Topology-reconfigurable capacitor matrix for encrypted dynamic wireless charging of electric vehicles. IEEE Transactions on Vehicular Technology, 67(10), 9284-9293.

[7] Khouri, K. (2018, March). Keynote abstract: Safety and security at the heart of autonomous driving. In 2018 1st Workshop on Energy Efficient Machine Learning and Cognitive Computing for Embedded Applications (EMC2) (pp. 1-1). IEEE.

[8] Bomfim, T. S. (2020, August). Evolution of machine learning in smart grids. In 2020 IEEE 8th International Conference on Smart Energy Grid Engineering (SEGE) (pp. 82-87). IEEE.

[9] Malik, R. Q., Alsattar, H. A., Ramli, K. N., Zaidan, B. B., Zaidan, A. A., Kareem, Z. H., ... & Zaidan, R. A. (2019). Mapping and deep analysis of vehicle-to-infrastructure communication systems: Coherent taxonomy, datasets, evaluation and performance measurements, motivations, open challenges, recommendations, and methodological aspects. IEEE Access, 7, 126753-126772.

[10] Biron, Z. A., Dey, S., & Pisu, P. (2018). Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Transactions on Intelligent Transportation Systems, 19(12), 3893-3902.

[11] Lv, Z., Qiao, L., Cai, K., & Wang, Q. (2020). Big data analysis technology for electric vehicle networks in smart cities. IEEE Transactions on Intelligent Transportation Systems, 22(3), 1807-1816.

[12] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access, 8, 23817-23837.

[13] Kim, T., Ochoa, J., Faika, T., Mantooth, H. A., Di, J., Li, Q., & Lee, Y. (2020). An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE Journal of Emerging and

Selected Topics in Power Electronics, 10(1), 1270-1281.

[14] Gunapriya Balan, Singaravelan Arumugam, Suresh Muthusamy, Hitesh Panchal, Mohit Bajaj, Hossam Kotb, Sherif S. M. Ghoneim, Kitmo. "An improved deep learning based technique for driver detection and driver assistance in electric vehicles with better performance." International Transactions on Electrical Energy Systems, vol. 2022, Article ID 8548172, 16 pages, 2022. https://doi.org/10.1155/2022/8548172.

[15] Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D., & Douligeris, C. (2022). Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Communications Surveys & Tutorials.

[16] Bhatti, G., Mohan, H., & Singh, R. R. (2021). Towards the future of smart electric vehicles: Digital twin technology. Renewable and Sustainable Energy Reviews, 141, 110801.

[17] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

[18] Mohamed, N. (2022, December). Importance of Artificial Intelligence in Neural Network through using MediaPipe. In 2022 6th International Conference on Electronics, Communication and Aerospace Technology (pp. 1207-1215). IEEE.

[19] Mohamed, N., & Belaton, B. (2021). SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique. IEEE Access, 9, 42919-42932.

[20] Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. Heliyon, 4(11), e00938.

[21] Mohamed, N. A., Jantan, A., & Abiodun, O. I. (2018). An improved behaviour specification to stop advanced persistent threat on governments and organizations network. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1, pp. 14-16).

[22] Ma, Y., Wang, Z., Yang, H., & Yang, L. (2020). Artificial intelligence applications in the development of autonomous vehicles: a survey. IEEE/CAA Journal of Automatica Sinica, 7(2), 315-329.

[23] Sharma, P., & Gillanders, J. (2022). Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art. IEEE Access.

[24] Mohamed, N., Alam, E., & Stubbs, G. L. (2022). Multi-layer protection approach (MLPA) for the detection of advanced persistent threat. Journal of Positive School Psychology, 4496-4518.

[25] Omolara, A. E., Jantan, A., Abiodun, O. I., Arshad, H., & Mohamed, N. A. (2019). Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication. International Journal of Electrical & Computer Engineering, 9(3).

[26] Mohamed, N. (2022). State-of-the-Art in Chinese APT Attack and Using Threat Intelligence for Detection. A Survey. Journal of Positive School Psychology, 4419-4443.

[27] Mohamed, N., Almazrouei, S. K., Oubelaid, A., Elsisi, M., ElHalawany, B. M., & Ghoneim, S. S. (2022). Air-Gapped Networks: Exfiltration without Privilege Escalation for Military and Police Units. Wireless Communications and Mobile Computing, 2022.

[28] Mohamed, N., Awasthi, A., Kulkarni, N., Thota, S., Singh, M., & Dhole, S. V. (2022). Decision Tree Based Data

Pruning with the Estimation of Oversampling Attributes for the Secure Communication in IoT. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 212-216.