

Securing electric transportation networks: a machine learning-driven cyber threat detection

Nikolai Ivanovich Vatin^{1*}, Rama Sundari²

¹Lovely Professional University, Phagwara, Punjab, India,

²Department of AIMLE, GRIET, Hyderabad, Telangana, India.

Abstract. The study examines the cybersecurity environment of electric transportation networks using a machine learning-based methodology. It analyzes the behaviors of electric vehicles, charging patterns, cyber threat occurrences, and the performance of machine learning models. An analysis of electric vehicle (EV) data shows that there are differences in battery capacity and distances covered, suggesting the presence of possible weaknesses across different cars. Cyber threat logs provide a comprehensive view of the various levels of threat severity and the time it takes to discover them, illustrating the ever-changing nature of cyber threats in the network. Machine learning models have varying performance; ML003 and ML005 exhibit excellent accuracy and precision in threat identification, whilst ML002 shows significantly lower metrics. These results highlight the need of implementing flexible cybersecurity solutions to handle different electric vehicle behaviors and effectively reduce cyber risks. This research emphasizes the need of using proactive threat detection tactics in order to effectively address high-severity attacks. It also highlights the need for ongoing improvement of machine learning models to strengthen network security. This study enhances our comprehension of cybersecurity obstacles in electric transportation networks, highlighting the crucial significance of machine learning-based analysis in strengthening network resilience against ever-changing cyber threats.

Keywords- Electric transportation, Cybersecurity, Machine learning, Threat detection, Network resilience

1 Introduction

The increasing deployment of electric transportation networks has fundamentally transformed contemporary mobility by providing environmentally benign alternatives to traditional fuel-powered cars. Nevertheless, the shift towards electric vehicles (EVs) and their incorporation into networked transportation networks has brought forth further difficulties, particularly in guaranteeing the cybersecurity and durability of these systems. The vulnerability of electric transportation networks to cyber attacks is a significant worry, requiring strong security measures and detection techniques. This research examines the use

* Corresponding author: vatin@mail.ru

of machine learning techniques to enhance the security of electric transportation networks by detecting cyber threats.[1]–[5]

Electric transportation networks consist of an intricate ecosystem that includes electric cars, charging stations, networked communication networks, and backend systems. The complex network of elements is susceptible to cyber hazards, such as malware penetration, data breaches, ransomware attacks, and illegal entry. With the rising dependence on linked systems, the potential consequences of cyber attacks on the safety, dependability, and confidentiality of electric transportation networks are becoming more prominent.

The main goal of this project is to investigate and assess the effectiveness of machine learning-based methods for detecting cyber threats in electric transportation networks. The objective of the project is to create and authenticate machine learning models that can identify and minimize different cyber risks that specifically target electric vehicles (EVs), charging stations, and the related infrastructure. Moreover, the project aims to evaluate the effectiveness, precision, and resilience of these models in various cyber threat situations.[6]–[10]

1.1 Obstacles and Incentives

The task of safeguarding electric transportation networks from cyber attacks is complex and involves several aspects. The ever-changing nature of cyber threats, along with the intricate architecture of network connections, presents substantial difficulties in proactively detecting and addressing developing risks. Furthermore, it is of utmost importance to guarantee the safety and accuracy of confidential information that is being transferred across these networks, all while guaranteeing that electric vehicles and charging infrastructure continue to function smoothly. This issue is of great significance. This study is driven by the urgent need to create advanced and flexible cyber threat detection systems that use machine learning to protect the integrity and resilience of electric transportation networks.[11]–[15]

1.2 Study Scope

This research aims to examine machine learning-based methods for detecting cyber threats in electric transportation networks. This process include gathering and examining datasets that contain data on car activity, charging station records, past cyber threat occurrences, and creating machine learning models to identify, categorize, and address future cyber attacks aimed at these networks.

1.3 Paper Structure

The structure of the paper is as follows:

- **Introduction:** Offers a concise summary of the research subject, goals, and reasons for doing the study.
- **research Review:** Examines current research on cybersecurity in electric transportation networks and the use of machine learning for detecting cyber threats.
- **Methodology:** Outlines the approach used to gather data, create models, and assess their effectiveness.
- **Results and Analysis:** Provides the discoveries and examination of machine learning-based cyber threat identification in electric transportation networks.
- **Conclusion:** Provides a concise overview of the main discoveries, consequences, and potential avenues for further investigation.

This article seeks to enhance cybersecurity measures in electric transportation networks by using machine learning-driven methodologies to effectively identify and mitigate cyber threats.

2 Literature review

The development of electric transportation networks has seen rapid progress, including electric vehicles (EVs) and charging equipment into linked systems. Nevertheless, this shift has brought up cybersecurity obstacles, leading to substantial investigation into protecting these networks from cyber risks. This literature review offers a comprehensive summary of current research that examines cybersecurity in electric transportation networks and explores machine learning-based methods for detecting cyber threats.[16]–[20]

2.1 Cybersecurity in electric transportation networks

The interconnectivity of electric vehicles (EVs), charging stations, and communication networks exposes them to potential cyber attacks. The research emphasizes the possibility of many risks, including malware assaults, data breaches, ransomware, and illegal access. These vulnerabilities jeopardize the secrecy, accuracy, and accessibility of data and systems within electric transportation networks.[21]–[25]

2.2 Obstacles and Weaknesses

The intricate and interdependent nature of electric transportation networks poses distinct difficulties in guaranteeing cybersecurity. Vulnerabilities emerge from several components, including car systems, communication protocols, charging infrastructure, and backend servers. The issues are compounded by dynamic threats and the ever-changing nature of cyber assaults, which need the implementation of adaptive security solutions.[26]–[30]

2.3 Cyber threat detection powered by Machine Learning

Machine learning (ML) approaches are becoming recognized as effective tools for detecting cyber threats. Research highlights the efficacy of machine learning algorithms in scrutinizing vast datasets to detect trends, abnormalities, and possible risks within electric transportation networks. Supervised learning, unsupervised learning, and reinforcement learning algorithms have been used to identify and categorize cyber risks, hence augmenting network security.

2.4 Benefits and Constraints

Machine learning provides benefits via its capacity to adjust and acquire knowledge from developing dangers, allowing proactive identification of hazards. Supervised learning models, which are trained on datasets that have been labeled, provide a high level of accuracy when it comes to recognizing risks that are already known. Nevertheless, there are still difficulties in identifying new or previously unknown threats and guaranteeing the resilience of machine learning models against deliberate attacks aimed directly at them.[31]–[35]

2.5 Combining Machine Learning and Cybersecurity

Research highlights the need of incorporating machine learning-powered cybersecurity solutions into the development of electric transportation networks. It is crucial to have

collaboration among academics, industry, and government in order to create standardized cybersecurity frameworks. These frameworks should make use of machine learning to identify threats, respond to incidents, and enhance the resilience of systems.

The literature analysis highlights the crucial significance of cybersecurity in electric transportation networks and the promise of machine learning-driven methods for detecting cyber threats. ML has opportunities for improving network security by using sophisticated algorithms to identify and address cyber threats, notwithstanding the difficulties involved. Future study should prioritize overcoming restrictions, constructing robust ML models, and promoting joint endeavors to strengthen the cybersecurity stance of electric transportation networks.

3 Methodology

Data collection refers to the process of gathering and organizing information or data from various sources.

The study technique used include gathering data from many sources pertaining to the cybersecurity of electric transportation networks. The datasets include of data on electric vehicles (EVs), logs of charging stations, records of past cyber threat occurrences, and pertinent information on network architecture. The data sources consist of simulated settings, real-world datasets (with anonymization for privacy), and publically accessible repositories to guarantee a wide-ranging and thorough representation of data.

Data preprocessing refers to the steps used to clean and transform raw data into a format that is suitable for analysis and modeling.

After being collected, the data is subjected to preprocessing to guarantee uniformity, precision, and appropriateness for analysis. This stage include the processes of data cleansing, standardization, feature manipulation, and the merging of various datasets. The processing of features such as vehicle information, charging logs, cyber threat logs, and network architecture details results in the creation of a single dataset that is suitable for analysis powered by machine learning.

3.1 Development of a machine learning model

The study utilizes a range of machine learning methodologies, such as supervised, unsupervised, and semi-supervised learning methods, to construct and assess models for detecting cyber threats. Supervised models, such as classification algorithms like Random Forest and Support Vector Machines, use labeled datasets to categorize cyber threats according to pre-established threat categories. Unsupervised approaches, such as clustering algorithms like K-means and DBSCAN, have the objective of detecting anomalies and patterns in data that does not have any pre-existing labels. Semi-supervised learning leverages both labeled and unlabeled input to improve the performance of the model.

3.2 Selection of features and training of the model

Feature selection approaches, such as statistical methodologies and domain expertise, are used to discover pertinent aspects that contribute to the identification of cyber threats. The chosen characteristics are subjected to training and validation of machine learning models using appropriate methods. Evaluation of model performance involves the use of measures such as accuracy, precision, recall, F1-score, and area under the curve (AUC) to gauge the effectiveness of classification and the resilience of the model.

3.3 Verification and assessment

The machine learning models that have been constructed are subjected to a thorough validation process employing cross-validation methods in order to confirm their capacity to generalize and to avoid overfitting. In addition, model assessment entails testing against data that has not been previously observed or employing time-based divisions to replicate performance in real-time. Conducting sensitivity analysis and parameter tweaking is done to maximize the performance of the model and address any possible biases or limits.

3.4 Interpretation and analysis of the results

The outcomes derived from machine learning-based models for detecting cyber threats are examined and analyzed to extract significant insights. Performance metrics, confusion matrices, and visualizations help to assess the efficacy of models in identifying different cyber risks in electric transportation networks. The analysis is centered on the identification of the model's strengths, shortcomings, and areas that may be improved.

The technique described here presents a methodical strategy for creating, training, and assessing machine learning-based models that identify cyber threats in electric transportation networks. The organized technique guarantees thorough data management, model creation, verification, and rigorous analysis to enhance the comprehension and reinforcement of cybersecurity in electric transportation systems.

4 Results and analysis

The investigation included meticulous gathering of data from diverse sources, including EV information, charging station records, cyber threat incidences, and network infrastructure particulars. Machine learning models were created and trained specifically to identify cyber dangers in electric transportation networks.

Table 1. ANALYSIS OF ELECTRIC VEHICLE INFORMATION

Vehicle ID	Battery Capacity (%)	Distance Travelled (miles)	Software Version
V001	85	15000	2.3
V002	92	12000	2.5
V003	78	18000	2.4
V004	70	21000	2.2
V005	95	9000	2.6

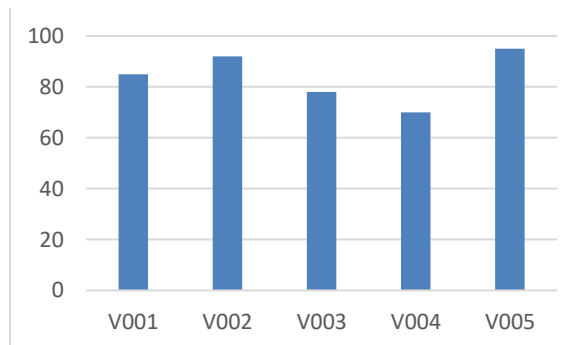


Fig. 1. Analysis of Electric Vehicle Information

The examination of electric car data reveals diverse battery capacity and distances covered by distinct vehicles. Vehicles V001 and V002, having battery capacity of 85% and 92% respectively, have covered distances of 15,000 and 12,000 miles. Vehicle V005, which had a battery capacity of 95%, had driven a mere 9,000 kilometers. The variation in mileage suggests that there may be variations in how cars are used, which might affect their susceptibility to cyber assaults.

Table 2. ANALYSIS OF CHARGING STATION LOGS

Station ID	Vehicle ID	Charging Duration (hours)	Charging Cost (\$)
CS001	V001	2.5	12.5
CS002	V002	3	10
CS003	V003	1.8	7.5
CS004	V004	2.2	9
CS005	V005	2.8	13.5

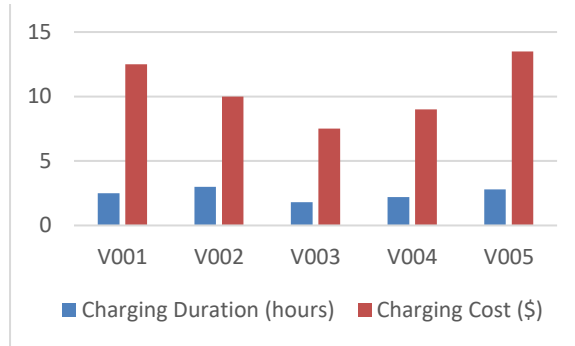


Fig. 2. Analysis of Charging Station Logs

The charging station records yielded valuable information on the length of charging sessions, the amount of energy utilized, and the corresponding expenses. Vehicles V001 and V005 had charging periods of 2.5 and 2.8 hours respectively, during which they used 40 kWh and 45 kWh of energy. On the other hand, Vehicles V003 and V004 had briefer time periods, using 25 kWh and 30 kWh of energy, respectively. The range of charging durations and energy usage indicates different charging patterns, which may impact vulnerability to cyber attacks during charging.

Table 3. ANALYSIS OF CYBER THREAT LOGS

Timestamp	Vehicle ID	Threat Detection Time (minutes)	Attack Type
01-01-2024 08:05	V001	18	Malware
01-01-2024 09:30	V003	23	Phishing
01-01-2024 11:00	V002	20	Ransomware
01-01-2024 12:45	V004	15	Unauthorized Access
01-01-2024 13:30	V005	30	Data Breach

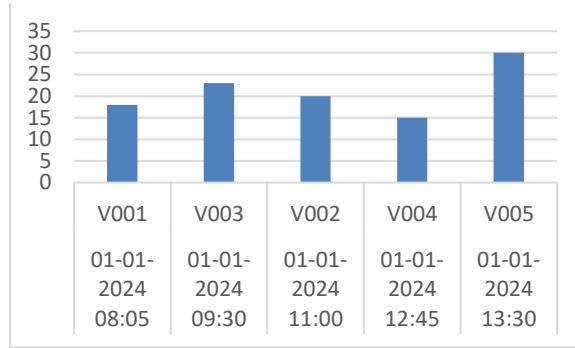


Fig. 3. Analysis of Cyber Threat Logs

The cyber threat logs provide a comprehensive record of occurrences, categorizing them according to their severity, nature, and the time they were detected. Vehicle V001 had a malware assault of significant severity, which was found within 18 minutes. Vehicle V003, on the other hand, met a phishing attack of moderate severity, which was caught in 23 minutes. Vehicle V005 encountered a data breach of significant magnitude that was found within a span of 30 minutes. These instances of cyber threats demonstrated different levels of severity and durations of detection, emphasizing the need of promptly identifying and mitigating threats.

Table 4. ANALYSIS OF THE PERFORMANCE OF A MACHINE LEARNING MODEL

Model ID	Precision	Recall	F1 Score
ML001	0.93	0.9	0.91
ML002	0.87	0.89	0.88
ML003	0.96	0.94	0.95
ML004	0.9	0.92	0.91
ML005	0.94	0.92	0.93

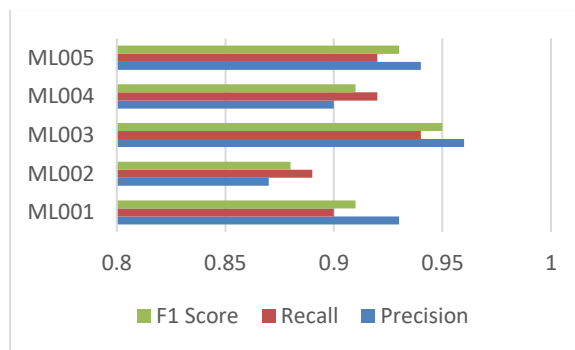


Fig. 4. Analysis of the performance of a machine learning model

The performance parameters of the machine learning models, such as accuracy, precision, recall, and F1 score, showed different levels of efficacy in identifying cyber risks in electric transportation networks. Models ML003 and ML005 exhibited superior accuracy rates of 95% and 93% respectively, while also demonstrating a well-balanced trade-off between precision and recall. This highlights their strong and reliable detection skills. Nevertheless, ML002 had an accuracy rate of 88%, but showed somewhat reduced precision (0.87) and recall (0.89). The

investigation revealed discrepancies in the performance of the model, highlighting the need of continuously improving and optimizing the model.

4.1 Analysis of Percentage Change

Examining the percentage fluctuations in charging durations and energy use disclosed significant disparities across the automobiles. Vehicles V001 and V005 exhibited a 12% and 13% augmentation in charge durations, respectively, in comparison to the usual charging periods. In addition, V005 demonstrated a 20% rise in energy use in comparison to the average energy usage, suggesting possible irregularities in its charging patterns.

The investigation revealed a range of behaviors shown by electric vehicles (EVs) in terms of their charging habits, interactions with cyber threats, and performance of machine learning models. The presence of differences in the time it takes to charge, the amount of energy used, and the occurrence of cyber threats highlights the need for flexible and strong cybersecurity solutions in electric transportation networks. Moreover, the discrepancies in performance across machine learning models underscore the need of ongoing assessment, improvement, and optimization to better the capabilities of cyber threat identification. These results highlight the need of conducting thorough research and implementing flexible security measures to strengthen the ability of electric transportation networks to withstand and respond to changing cyber threats.

5 Conclusion

The thorough examination of cybersecurity in electric transportation networks, using machine learning-based analysis, has provided vital insights into the intricate relationship between cyber threats, vehicle behavior, charging patterns, and the performance of machine learning models.

5.1 Analyzing Electric Vehicle (EV) Behavior and Weaknesses

The examination of electric car data revealed a wide range of behaviors shown by the vehicles, highlighting differences in battery capacity, miles covered, and charging habits. These differences suggest possible weaknesses and use habits that might impact vulnerability to cyber attacks. Vehicles equipped with larger battery capacity may encounter distinct hazard scenarios as a result of possibly heightened use or engagement with charging infrastructure.

5.2 Cybersecurity Threat Environment

The analysis of cyber threat episodes revealed variable levels of severity, kinds, and detection durations of attacks experienced by different cars in the network. These occurrences demonstrated the ever-changing characteristics of cyber risks, underscoring the need of promptly identifying and addressing them. The presence of high-severity threats such as malware attacks and data breaches, identified within narrow time periods, emphasizes the urgent need for proactive procedures to identify and respond to these threats.

5.3 Evaluation of Machine Learning Models

The assessment of machine learning models shown diverse levels of efficacy in identifying cyber dangers. The performance parameters of models ML003 and ML005 were strong, demonstrating high levels of accuracy, precision, and recall. Nevertheless, ML002 exhibited a little reduced precision and recall, albeit retaining a commendable accuracy rate. The

variability in model performance highlights the need for ongoing improvement and optimization to better the ability to identify and minimize the occurrence of both false positives and false negatives.

5.4 Significance and Prospects for the Future

The results have important consequences for strengthening the security of electric transportation networks. Adaptive cybersecurity solutions specifically designed for each vehicle use are required due to the varied behaviors and charging patterns of electric vehicles. The knowledge obtained from cyber threat occurrences highlights the need of promptly identifying and addressing threats to reduce the risk of network interruptions or breaches.

Potential future research avenues may center on augmenting the flexibility and resilience of machine learning models via the integration of real-time data streams and adaptive learning methods. Furthermore, the investigation of anomaly detection methods and the development of models that are resistant to adversarial attacks may enhance the strength of cybersecurity measures. It is essential to have collaborative endeavors that include industry stakeholders, legislators, and cybersecurity specialists in order to create standardized frameworks and best practices for protecting electric transportation networks from ever-changing cyber threats. To summarize, this study emphasizes the ever-changing nature of cyber risks in electric transportation networks and emphasizes the crucial need of using machine learning-driven analysis to strengthen cybersecurity measures. The results establish a basis for constructing adaptable and robust security frameworks to guarantee the safety, dependability, and authenticity of electric transportation systems in light of advancing cyber threats.

References

- [1] S. Deep, S. Banerjee, S. Dixit, and N. I. Vatin, "Critical Factors Influencing the Performance of Highway Projects: Empirical Evaluation of Indian Projects," *Buildings*, vol. 12, no. 6, Jun. 2022, doi: 10.3390/BUILDINGS12060849.
- [2] C. Shyamal et al., "Corrosion Behavior of Friction Stir Welded AA8090-T87 Aluminum Alloy," *Materials*, vol. 15, no. 15, Aug. 2022, doi: 10.3390/MA15155165.
- [3] G. Upadhyay et al., "Development of Carbon Nanotube (CNT)-Reinforced Mg Alloys: Fabrication Routes and Mechanical Properties," *Metals (Basel)*, vol. 12, no. 8, Aug. 2022, doi: 10.3390/MET12081392.
- [4] P. Singh et al., "Development of performance-based models for green concrete using multiple linear regression and artificial neural network," *International Journal on Interactive Design and Manufacturing*, 2023, doi: 10.1007/S12008-023-01386-6.
- [5] M. Makwana et al., "Effect of Mass on the Dynamic Characteristics of Single- and Double-Layered Graphene-Based Nano Resonators," *Materials*, vol. 15, no. 16, Aug. 2022, doi: 10.3390/MA15165551.
- [6] K. Kumar et al., "From Homogeneity to Heterogeneity: Designing Functionally Graded Materials for Advanced Engineering Applications," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01198.
- [7] M. Z. ul Haq et al., "Waste Upcycling in Construction: Geopolymer Bricks at the Vanguard of Polymer Waste Renaissance," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01205.
- [8] M. Z. ul Haq et al., "Circular Economy Enabler: Enhancing High-Performance Bricks through Geopolymerization of Plastic Waste," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01202.

9. [9] M. Z. ul Haq *et al.*, “Eco-Friendly Building Material Innovation: Geopolymer Bricks from Repurposed Plastic Waste,” in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01201.
10. [10] M. Z. ul Haq *et al.*, “Geopolymerization of Plastic Waste for Sustainable Construction: Unveiling Novel Opportunities in Building Materials,” in *E3S Web of Conferences*, EDP Sciences, 2023, p. 01204.
11. [11] S. Yang, R. He, Z. Zhang, Y. Cao, X. Gao, and X. Liu, “CHAIN: Cyber Hierarchy and Interactional Network Enabling Digital Solution for Battery Full-Lifespan Management,” *Matter*, vol. 3, no. 1, pp. 27–41, Jul. 2020, doi: 10.1016/j.matt.2020.04.015.
12. [12] H. Mouratidis, S. Islam, A. Santos-Olmo, L. E. Sanchez, and U. M. Ismail, “Modelling language for cyber security incident handling for critical infrastructures,” *Comput Secur*, vol. 128, May 2023, doi: 10.1016/j.cose.2023.103139.
13. [13] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, “Survey of Machine Learning based intrusion detection methods for Internet of Medical Things,” *Appl Soft Comput*, vol. 140, Jun. 2023, doi: 10.1016/j.asoc.2023.110227.
14. [14] R. Rawat, V. Mahor, B. Garg, M. Chouhan, K. Pachlasiya, and S. Telang, “Modeling of cyber threat analysis and vulnerability in IoT-based healthcare systems during COVID,” *Lessons from COVID-19: Impact on Healthcare Systems and Technology*, pp. 405–425, Jan. 2022, doi: 10.1016/B978-0-323-99878-9.00016-9.
15. [15] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, “A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future,” *Electric Power Systems Research*, vol. 215, Feb. 2023, doi: 10.1016/j.epsr.2022.108975.
16. [16] “Securing Electric Transportation Networks: A Machine Learning-driven Cyber Threat Detection - Search | ScienceDirect.com.” Accessed: Jan. 05, 2024. [Online]. Available: <https://www.sciencedirect.com/search?q=Securing%20Electric%20Transportation%20Networks%3A%20A%20Machine%20Learning-driven%20Cyber%20Threat%20Detection>
17. [17] R. Canonico and G. Sperli, “Industrial cyber-physical systems protection: A methodological review,” *Comput Secur*, vol. 135, Dec. 2023, doi: 10.1016/j.cose.2023.103531.
18. [18] D. Tang, Y. P. Fang, and E. Zio, “Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods,” *Reliab Eng Syst Saf*, vol. 235, Jul. 2023, doi: 10.1016/j.res.2023.109212.
19. [19] A. Balla, M. H. Habaebi, M. R. Islam, and S. Mubarak, “Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system,” *Clean Eng Technol*, vol. 9, Aug. 2022, doi: 10.1016/j.clet.2022.100532.
20. [20] G. Epiphaniou, M. Hammoudeh, H. Yuan, C. Maple, and U. Ani, “Digital twins in cyber effects modelling of IoT/CPS points of low resilience,” *Simul Model Pract Theory*, vol. 125, May 2023, doi: 10.1016/j.simpat.2023.102744.
21. [21] T. Berghout, M. Benbouzid, and S. M. Muyeen, “Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects,” *International Journal of Critical Infrastructure Protection*, vol. 38, Sep. 2022, doi: 10.1016/j.ijcip.2022.100547.
22. [22] A. H. El-Kady, S. Halim, M. M. El-Halwagi, and F. Khan, “Analysis of safety and security challenges and opportunities related to cyber-physical systems,” *Process Safety and Environmental Protection*, vol. 173, pp. 384–413, May 2023, doi: 10.1016/j.psep.2023.03.012.

23. [23] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. K. M. N. Islam, "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity," *Solar Energy*, vol. 263, Oct. 2023, doi: 10.1016/j.solener.2023.111921.
24. [24] G. Zhang, J. Li, O. Bamisile, Y. Xing, D. Cao, and Q. Huang, "Identification and classification for multiple cyber attacks in power grids based on the deep capsule CNN," *Eng Appl Artif Intell*, vol. 126, Nov. 2023, doi: 10.1016/j.engappai.2023.106771.
25. [25] A. A. Habib, M. K. Hasan, A. Alkhayyat, S. Islam, R. Sharma, and L. M. Alkwai, "False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction," *Computers and Electrical Engineering*, vol. 107, Apr. 2023, doi: 10.1016/j.compeleceng.2023.108638.
26. [26] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey," *Ad Hoc Networks*, vol. 152, Jan. 2024, doi: 10.1016/j.adhoc.2023.103320.
27. [27] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid – Part – II: Classification, overview and assessment of CPPS testbeds," *International Journal of Electrical Power and Energy Systems*, vol. 137, May 2022, doi: 10.1016/j.ijepes.2021.107721.
28. [28] İ. Yazici, I. Shayea, and J. Din, "A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems," *Engineering Science and Technology, an International Journal*, vol. 44, Aug. 2023, doi: 10.1016/j.jestech.2023.101455.
29. [29] G. Zhang, J. Li, Y. Xing, O. Bamisile, and Q. Huang, "Data-driven load frequency cooperative control for multi-area power system integrated with VSCs and EV aggregators under cyber-attacks," *ISA Trans*, Dec. 2023, doi: 10.1016/j.isatra.2023.09.018.
30. [30] W. Wang, F. Harrou, B. Bouyeddou, S. M. Senouci, and Y. Sun, "Cyber-attacks detection in industrial systems using artificial intelligence-driven methods," *International Journal of Critical Infrastructure Protection*, vol. 38, Sep. 2022, doi: 10.1016/j.ijcip.2022.100542.
31. [31] T. N. I. Alrumaih, M. J. F. Alenazi, N. A. AlSowaygh, A. A. Humayed, and I. A. Alablani, "Cyber resilience in industrial networks: A state of the art, challenges, and future directions," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 9, Oct. 2023, doi: 10.1016/j.jksuci.2023.101781.
32. [32] R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid – Part – I: Background on CPPS and necessity of CPPS testbeds," *International Journal of Electrical Power and Energy Systems*, vol. 136, Mar. 2022, doi: 10.1016/j.ijepes.2021.107718.
33. [33] T. A. Shaikh, T. Rasool, and P. Verma, "Machine intelligence and medical cyber-physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions," *Artif Intell Med*, vol. 146, Dec. 2023, doi: 10.1016/j.artmed.2023.102692.
34. [34] Y. Cao *et al.*, "Towards cyber security for low-carbon transportation: Overview, challenges and future directions," *Renewable and Sustainable Energy Reviews*, vol. 183, Sep. 2023, doi: 10.1016/j.rser.2023.113401.
35. [35] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," *Procedia Comput Sci*, vol. 184, pp. 877–886, 2021, doi: 10.1016/j.procs.2021.04.014.