

Cyber-physical resilience system for anomaly detection in industrial environments

Debani Prasad Mishra¹, Rakesh Kumar Lenka², Rampa Sri Sai Yagyna Duthsharma¹,
Pavan Kumar¹, Lakshay Bhardwaj¹, Surender Reddy Salkuti³

¹Department of Electrical Engineering, IIIT Bhubaneswar, Odisha, India

²Department of Computer Science, Central University of Odisha, India

³Department of Railroad and Electrical Engineering, Woosong University, Daejeon, Republic of Korea

Article Info

Article history:

Received Jun 4, 2024

Revised Dec 17, 2024

Accepted Jan 19, 2025

Keywords:

Anomaly detection

Cyber-physical resilience

Monitoring system

Multithreading

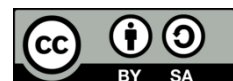
Real-time detection

Response protocol

ABSTRACT

This work explores the topic of cybersecurity in the context of electric vehicles (EVs). It ensures the resilience of cyber-physical systems against anomalies, which is paramount for maintaining operational efficiency and safety. This paper presents a cyber-physical resilience system (CPRS) customized for anomaly detection. Maintaining operational efficiency and safety in today's networked industrial contexts requires that cyber-physical systems be resilient to abnormalities. With an emphasis on EVs, this research introduces a unique CPRS designed for anomaly detection in industrial settings. By utilizing the combination of digital and physical elements, the CPRS uses sophisticated monitoring and reaction systems to identify and address irregularities instantly. The process includes creating algorithms for anomaly detection and putting in place a framework that is responsive enough to change with the dangers that it faces. The efficiency of the CPRS in detecting unusual behaviors in EVs is demonstrated by experimental findings, which also improve the overall resilience of the system. Moreover, the research's ramifications go beyond EVs to include a variety of industrial settings, providing valuable information for the development and execution of resilient cyber-physical systems. This paper highlights the significance of proactive resilience measures in protecting critical infrastructure and advances anomaly detection approaches.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Surender Reddy Salkuti

Department of Railroad and Electrical Engineering, Woosong University

Jayang-Dong, Dong-Gu, Daejeon 34606, Republic of Korea

Email: surender@wsu.ac.kr

1. INTRODUCTION

An advanced electrical distribution network that integrates several technologies to improve the power grid's sustainability, dependability, and efficiency is referred to as a smart grid. Power generation, transmission, distribution, and consumption may exchange information and energy in both directions thanks to the utilization of communication, sensing, and control technology. Electricity stored in rechargeable batteries powers electric cars or electric vehicles (EVs). They have several benefits, including a lower carbon footprint and less reliance on fossil fuels. Plug-in hybrid electric cars (PHEVs), which combine an electric motor and an internal combustion engine, and battery electric vehicles (BEVs), which operate exclusively on electricity, are the two types of EVs. Importance of cybersecurity in smart grids and EVs [1]. Smart grids and EVs are becoming more and more integrated which raises new cybersecurity concerns and emphasizes how crucial it is to secure these systems. The importance of cybersecurity in these fields is demonstrated next.

System stability and reliability: smart grids are vital pieces of infrastructure that need to function consistently to provide a steady supply of electricity. Cyberattacks on smart grids have the potential to cause power distribution disruptions, which could result in blackouts, monetary losses, and even safety hazards. In data integrity and privacy, sensitive and personal data is generated and exchanged in large quantities by smart grids and EVs. Preventing unwanted access, data breaches, and exploitation requires safeguarding customer privacy and maintaining data integrity. And in EV safety and functionality, EVs' safety and functionality may be jeopardized by cybersecurity flaws [2]. Drivers, passengers, and other road users could be put in danger if malicious actors were to obtain unauthorized access to vehicle systems, alter controls, or interfere with the infrastructure that supports charging. Also in grid-to-vehicle (G2V) and vehicle-to-grid (V2G) interactions, since EVs are becoming more and more involved in grid operations, safe communication protocols and authentication techniques are crucial. Preventing unauthorized access to or manipulation of energy transactions is achieved by guaranteeing the integrity of these communications. Economic repercussions, utilities, transportation networks, and the national economy may all be significantly impacted by a successful cyberattack on smart grids or EV infrastructure. Safeguarding these systems against cyberattacks is essential for maintaining and expanding the economy. Strong cybersecurity measures are therefore necessary to protect sensitive data, prevent cyberattacks on smart grids and EVs, and guarantee the dependable and secure operation of these interconnected systems. These measures include threat monitoring, intrusion detection and prevention systems, encryption, authentication protocols, and security standards.

The following are the goals and scope of the literature review on cybersecurity in EVs and smart grids: throughout cybersecurity in smart grids, the evaluation focuses on the issues, risks, and fixes related to smart grid cybersecurity. It looks at possible cyberattacks, the threat landscape, and how they affect grid stability and dependability. Cybersecurity concerns with EVs delve into the cybersecurity challenges surrounding EVs, encompassing threats to EV charging infrastructure, possible intrusions on EVs and charging stations, and matters about data protection and privacy [3]. The data transmission process is illustrated in Figure 1. The data transmission process and visualization methods [4] with the integration of smart grids and EVs. This examines the cybersecurity implications of the interdependencies that exist between smart grids and EVs.

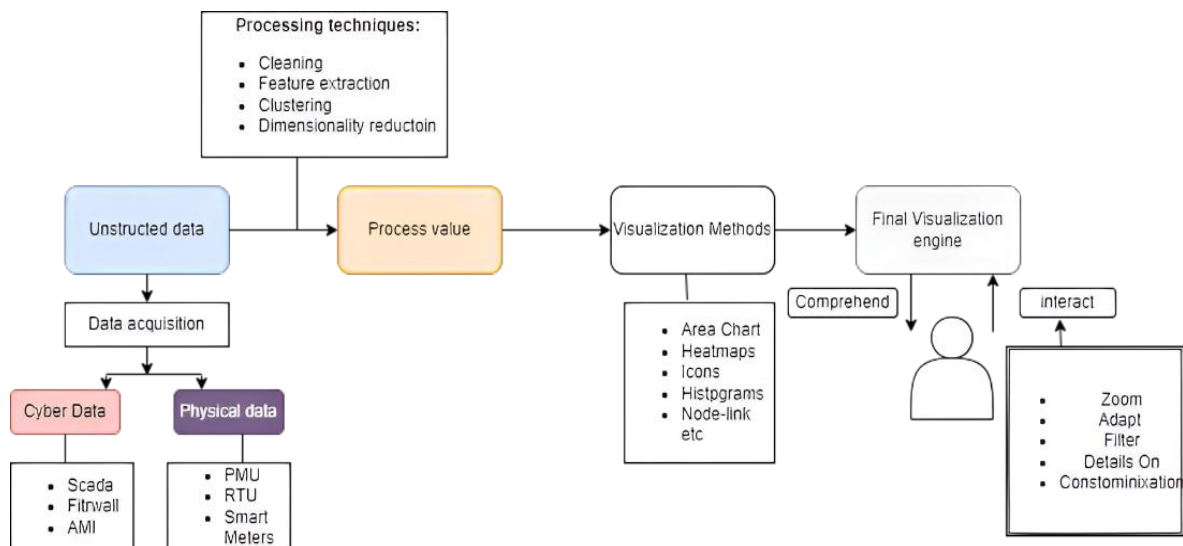


Figure 1. Data transmission process

It looks at the secure communication protocols and security issues for V2G and G2V connectivity. Determining cybersecurity challenges is the goal of the literature research, which is to determine and examine the cybersecurity issues and weaknesses unique to EVs and smart grids. It examines the dangers and hazards that these systems can encounter from illegal access, data breaches, and cyberattacks. A review of cybersecurity solutions looks at methods and solutions now in use for cybersecurity that are intended to lessen the issues that have been identified [5]. It examines security frameworks and standards relevant to EVs and smart grids, as well as intrusion detection and prevention systems, encryption, and authentication

methods. Emphasizing the future directions and challenges in the area of smart grid and EV cybersecurity, the evaluation seeks to highlight new developments, technologies, and research needs. It looks at the difficulties and future directions that will need to be addressed to improve these systems' security. The purpose of the literature review is to provide recommendations for improving cybersecurity in EVs and smart grids. These suggestions might cover topics for more study and development, regulatory actions, and policy ramifications. To maintain the safe and dependable operation of these interconnected systems, the literature review's overall goals are to present a thorough overview of the cybersecurity environment in smart grids and EVs, examine current solutions, and pinpoint areas that need improvement.

2. METHOD

Examination techniques for cyberattacks and the danger of EVs: cyberattack techniques for EVs cyberattack techniques are analyzed in terms of four distinct attack layers, with a diagram illustrating which attacks are possible in each tier. Taking precautions against such attacks is the goal here. Figure 2 depicts the EV cyber-attack techniques. EV security risk: because of economic fuel costs and environmental pollution, the usage of EVs is growing. In terms of security, risk becomes more apparent with this growth. This paper discusses the risk that could materialize if there is a security flaw in electric automobiles. These dangers include both taking on and accepting risks.

EV security risk assessment R-1: physical harm to the charging stations R-2: theft of client information; R-3: stealing card details at payment locations R-4: theft of important car information as a result of using unsecured data transmission methods R-5: customer data theft brought on by weaknesses in mobile applications International Exercise 13th Energy and Environment Symposium (IEEEES-13), Makkah, Saudi Arabia, November 15, 18, 2021 4 R-6: physical harm to automobiles and data alteration through cyberattacks on wireless networks R-7: data storage and application switching as a result of open USB ports R-8: turned off charging stations to prevent cyberattacks. R-9: to launch a brute-force cyberattack to obtain access to the Wi-Fi network that the users' home charger is connected to. R-10: is seizing command of the primary servers and remotely manipulating the car.

2.1. Vulnerable communication networks, data privacy, and protection

To exchange data and manage signals, smart grids, and EVs rely on communication networks. Unauthorized access, interception, and manipulation of these networks may result in the takeover of EVs or other grid components [6]. EVs and smart grids produce and share a lot of sensitive data, such as individual user profiles and energy usage trends. Protecting the privacy and security of data is essential to avoiding data breaches, unwanted access, and improper use of personal data.

2.2. Physical security risks and human aspects

Cyber risks and physical security are major concerns for EVs and smart grids. Risks related to physical security include theft, vandalism, and unauthorized access to vital infrastructure parts. Malicious actions of this kind have the potential to compromise system integrity, resulting in disruptions to operations and possibly serious repercussions for the functioning of vehicles and the electrical grid. To reduce these dangers, it is essential to have strong physical security measures in place, such as access control, monitoring, and tamper-resistant designs. Cybersecurity dangers are a significant risk to EVs and smart grids, in addition to physical threats. These may result from carelessness, malevolent purpose, or human error. Vulnerabilities may result from weak security procedures, ignorance, or inadequate training for system administrators, employees, and end users [7]. Comprehensive training programs, strict access controls, and frequent security audits to find and fix possible vulnerabilities are all essential components of effective cybersecurity plans.

Safeguarding smart grids and EVs requires a comprehensive security strategy that incorporates both physical and cyber defenses. Stakeholders can improve the robustness and dependability of these cutting-edge technologies and guarantee their safe and effective functioning in a world growing more linked by tackling these complex difficulties. Cyberattack methods in EVs are shown in Figure 2. It comprises strong cybersecurity measures, including encryption, authentication procedures, intrusion detection systems, security monitoring, and incident response procedures, which must be put in place to address these issues [8]. Establishing and enforcing comprehensive cybersecurity standards and policies for smart grids and EVs requires cooperation among stakeholders, including manufacturers, utilities, policymakers, and researchers. To detect and reduce new threats and vulnerabilities, regular security audits, vulnerability assessments, and continuous monitoring are also essential [9], [10].

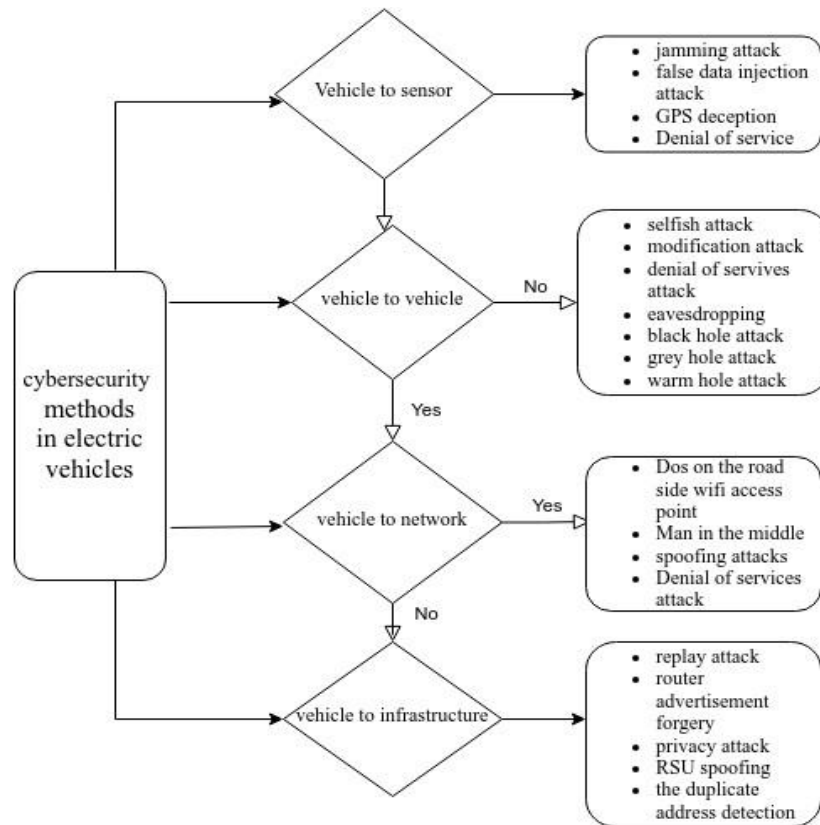


Figure 2. Cyber attack methods in EV

3. CYBERSECURITY SOLUTIONS FOR SMART GRIDS

3.1. Encryption, data protection, access control, and authentication

In smart grids, data transmission and storage are made secure using encryption techniques. Data encryption makes sure that information shared between systems and grid components is private and shielded from unwanted access. Robust encryption methods and algorithms, such as transport layer security (TLS) and advanced encryption standard (AES). Users and devices wishing to access the smart grid system are authenticated and granted permission through access control measures [11] that only authorized users may access vital systems and data, multi-factor authentication, strong password rules, and role-based access control (RBAC) are used. To guarantee that only authorized users may access vital systems and data, multi-factor authentication, strong password rules, and RBAC are used [12].

3.2. Security monitoring and incident response

Early detection of cyber threats is made possible by continuous security monitoring of the grid infrastructure. To detect any security problems, security information and event management (SIEM) [13] systems gather and examine security event logs, network traffic information, and system warnings. Plans and protocols for incident response facilitate quick and efficient reactions to lessen the effects of cyberattacks [14]. The whole composition, along with the structural process of identification of cyber threat by k-map cycle, is shown in Figure 3 with all blocks such as execution, target system, and monitoring. And planning, monitoring, and executing the targeted system, which is the anomaly or any cyber threat found by deep analysis [15], [16].

3.3. Supply chain security, security guidelines, and policies

To stop hostile or compromised components from infiltrating the infrastructure of the smart grid, supply chain security must be guaranteed. To create strong defenses and guarantee the safe and dependable operation of the grid infrastructure, utilities, suppliers, regulators, and cybersecurity specialists must work together [17]. Following numerous examples of cyberattacks, upon working on the following solution course, here's a basic recommendation for an electrical car cybersecurity app code, which is shown in Figure 4. It also gives us the detection of analyte and analysis by using the Mape K adaptation model [18], [19].

The code for anomaly detection is presented in Table 1. The ‘CybersecurityApp’ class, which is being defined in this example, encapsulates the functionality of keeping an eye on the electrical vehicle’s systems for any unusual or suspicious activity [20]. While the stop()’ function pauses the monitor and waits for the thread to finish, the start ()’ method launches a separate thread that continually checks the vehicle’s systems. The main function of the application is the monitor()’ method, where you can apply the logic to identify irregularities. To find possible cyber threats, this may entail examining network traffic, evaluating system records, or applying machine learning (ML) techniques. The ‘respond_to_anomaly ()’ function can be used to alert the user to a possible security risk if an anomaly is found [21], [22].

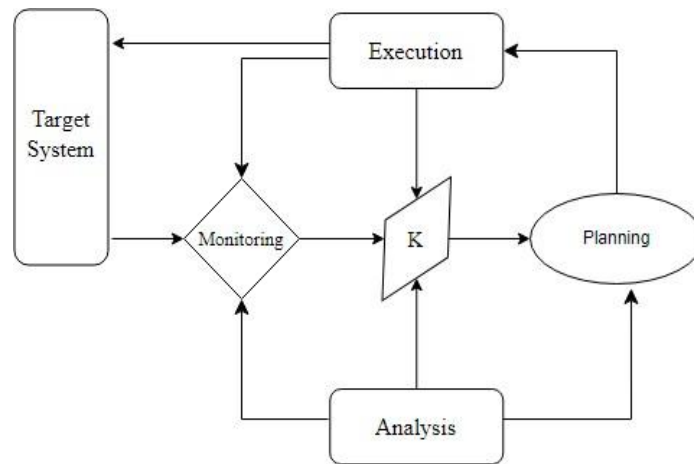


Figure 3. Identification of cyber threat by map k cycle

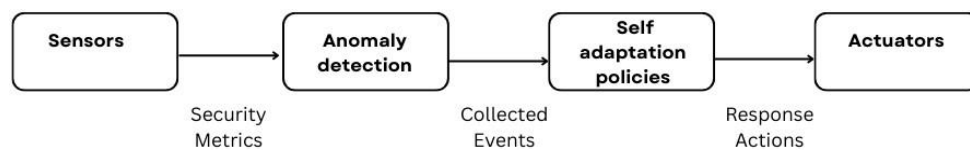


Figure 4. Anomaly detection to support monitoring and analysis in the MAPE-K adaptation model

Table 1. Code for anomaly detection

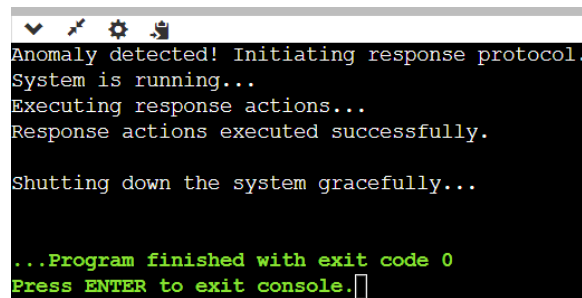
Code for anomaly	
1) Class CyberPhysicalResilienceSystem:	18) Print “Anomaly detected! Initiating response
2) Function init():	19) protocol.”
3) Initialize self.running to False	20) Execute_response_actions()
4) Function start():	21) Function execute_response_actions():
5) Set self.running to True	22) Print “Executing response actions...”
6) Start monitoring thread	23) Sleep for 2 seconds
7) Function stop():	24) Print “Response actions executed successfully.”
8) Set self.running to False	25) Main:
9) Join monitoring thread	26) Create instance of CyberPhysicalResilienceSystem
10) Function monitor():	27) Call start() on the instance
11) While self.running is True:	28) Try:
12) If detect_anomaly() is True:	29) Loop:
13) respond_to_anomaly()	30) Print “System is running...”
14) Sleep for 1 second	31) Sleep for 5 seconds
15) Function detect_anomaly():	32) On KeyboardInterrupt:
16) Return random choice of True/False	33) Print “Shutting down the system gracefully...”
17) Function respond_to_anomaly():	34) Call stop() on the instance

In this first part of the code, ‘import time’ provides functionality for time-related operations; ‘threading’ helps in working with threads; and finally, ‘random’ is used to generate random numbers for simulating anomalies. Secondly, a class named ‘cyberPhysicalResiliencesystem’ initializes with the Boolean attribute ‘running’, which indicates whether the system is running or not, and the start, stop, monitor, detect, and respond to anomalies are used for starting, stopping, and monitoring the anomalies, respectively [23].

4. DISCUSSION

The confluence of the cyber and physical domains makes ensuring the security of smart grids an ever-greater challenge. In this area, visualizations are essential for improving situational awareness, expediting decision-making, and spotting possible dangers. Nevertheless, integrating digital and physical data, reaching a comprehensive perspective, and facilitating interdisciplinary cooperation present considerable obstacles. Figure 5 explains the output part, which we obtained after successfully detecting and responding to the anomaly. The code is set to shut down the system gracefully.

The output of the code is the output of the above code, where, as it detects an anomaly, its response protocol is started and the status of the system is stated. After that, the response is executed, and once it is done successfully, it shuts down the system gracefully [24], [25]. Several specific cybersecurity techniques can be incorporated into the code for an electrical vehicle cybersecurity app. Here are a few examples:



```
Anomaly detected! Initiating response protocol.
System is running...
Executing response actions...
Response actions executed successfully.

Shutting down the system gracefully...

...Program finished with exit code 0
Press ENTER to exit console.█
```

Figure 5. Anomaly detection response protocol execution

4.1. Secure communication protocols and secure firmware updates

To provide encrypted and authenticated communication between the vehicle's components and external systems, implement secure communication protocols like TLS [26], [27]. This lessens the chance of interceptions, manipulation, and man-in-the-middle attacks. Implement secure mechanisms for updating the firmware of the vehicle's components. This can include digital signatures and secure boot processes to ensure the integrity and authenticity of firmware updates, preventing unauthorized modification.

4.2. Access control mechanisms and secure data storage

To limit and regulate user access to the systems and features of the car, put access control mechanisms in place. To prevent unwanted access, this can involve robust password restrictions, role-based access control, and user authentication. To safeguard stored sensitive information, use secure data storage techniques [28]. The confluence of the cyber and physical domains makes ensuring the security of smart grids an ever-greater challenge. In this area, visualizations are essential for improving situational awareness, expediting decision-making, and spotting possible dangers. Nevertheless, integrating digital and physical data, reaching a comprehensive perspective, and facilitating interdisciplinary cooperation present considerable obstacles. It appears from the output that was supplied that the cyber-physical resilience [29], [30] system was able to identify an anomaly, start the protocol, carry out the reaction activities, and shut down without incident.

The order in which these things happened suggests that the system functioned as planned and handled the anomaly as it was discovered. Along with the practical steps, the literature lines have also been checked. The system initiated its response protocol upon detecting an abnormality [31], [32]. Despite this, the notice "system is running" confirmed that the system was operating normally. Upon discovering the anomaly, the system executed response steps to address the identified problem, ultimately concluding its operations with a smooth shutdown [33]. Overall, the results demonstrate the effective implementation of the cyber-physical resilience system (CPRS), showcasing its ability to detect irregularities, respond appropriately, and maintain system integrity before carefully shutting down.

5. CONCLUSION

By utilizing artificial intelligence (AI)/ML innovations, encouraging interdisciplinary cooperation, and tackling data integration issues, smart grid security can be improved through sophisticated visualization techniques. In the future, extensive evaluation in real-world scenarios should be prioritized in order to

strengthen power grid resilience against dynamic threats. The CPRS is a vital tool for enhancing the resilience of industrial environments against rising threats and challenges. By embracing advanced technologies and proactive monitoring strategies, organizations can strengthen their defensive mechanisms, uphold operational continuity, and ultimately safeguard the integrity of critical infrastructure systems in the face of adversity. Industries to introduce digital transformation along with automation, which plays an important role in ensuring the reliability and stability of essential infrastructure components. These can increase the effectiveness and applicability of such things to real-life issues and problems.

FUNDING INFORMATION

This research work was supported by “Woosong University’s Academic Research Funding - 2025”.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Debani Prasad Mishra	✓	✓		✓	✓	✓	✓	✓		✓		✓	✓	
Rakesh Kumar Lenka				✓			✓	✓		✓		✓	✓	
Rampa Sri Sai Yagyna Duthsharma		✓	✓		✓	✓		✓	✓	✓	✓			
Pavan Kumar		✓	✓		✓	✓		✓	✓		✓			
Lakshay Bhardwaj		✓	✓		✓	✓		✓	✓	✓	✓			
Surender Reddy Salkuti				✓		✓	✓			✓		✓	✓	✓

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.





REFERENCES

- [1] X. Miao and X. Chen, “Cyber security infrastructure of smart grid communication system,” in *China International Conference on Electricity Distribution, CIGRE*, Sep. 2012, pp. 1–4, doi: 10.1109/CIGRE.2012.6508410.
- [2] Y. Wang, H. T. Luan, Z. Su, N. Zhang, and A. Benslimane, “A secure and efficient wireless charging scheme for electric vehicles in vehicular energy networks,” *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1491–1508, Feb. 2022, doi: 10.1109/TVT.2021.3131776.
- [3] M. M. Silveira *et al.*, “Data protection based on searchable encryption and anonymization techniques,” in *Proceedings of IEEE/IFIP Network Operations and Management Symposium 2023, NOMS 2023*, May 2023, pp. 1–5, doi: 10.1109/NOMS56928.2023.10154280.
- [4] V. Cobilean *et al.*, “A review of visualization methods for cyber-physical security: smart grid case study,” *IEEE Access*, vol. 11, pp. 59788–59803, 2023, doi: 10.1109/ACCESS.2023.3286304.
- [5] J. Ye *et al.*, “Cyber-physical security of powertrain systems in modern electric vehicles: vulnerabilities, challenges, and future visions,” *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021, doi: 10.1109/JESTPE.2020.3045667.
- [6] N. Saxena, V. Chukwuka, L. Xiong, and S. Grijalva, “CPSA: a cyber-physical security assessment tool for situational awareness in smart grid,” in *CPS-SPC 2017 - Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and Privacy, co-located with CCS 2017*, Nov. 2017, pp. 69–79, doi: 10.1145/3140241.3140246.
- [7] L. H. Fla, R. Borgeonkar, I. A. Tondel, and M. G. Jaatun, “Tool-assisted threat modeling for smart grid cyber security,” in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*, Jun. 2021, pp. 1–8, doi: 10.1109/CyberSA52016.2021.9478258.
- [8] J. Anu, R. Agrawal, C. Seay, and S. Bhattacharya, “Smart grid security risks,” in *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*, Apr. 2015, pp. 485–489, doi: 10.1109/ITNG.2015.84.
- [9] D. Said, M. Elloumi, and L. Khokhi, “Cyber-attack on P2P energy transaction between connected electric vehicles: a false data injection detection based machine learning model,” *IEEE Access*, vol. 10, pp. 63640–63647, 2022, doi: 10.1109/ACCESS.2022.3182689.




- [10] A. S. Mohamed, M. F. M. Arani, A. A. Jahromi, and D. Kundur, "False data injection attacks against synchronization systems in microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4471–4483, Sep. 2021, doi: 10.1109/TSG.2021.3080693.
- [11] D. Said and M. Elloumi, "A new false data injection detection protocol based machine learning for P2P energy transaction between CEVs," in *2022 IEEE International Conference on Electrical Sciences and Technologies in Maghreb, CISTEM 2022*, Oct. 2022, pp. 1–5, doi: 10.1109/CISTEM55808.2022.10044067.
- [12] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017, doi: 10.1109/TSG.2015.2495133.
- [13] N. Bhusal, M. Gautam, and M. Benidris, "Cybersecurity of electric vehicle smart charging management systems," in *2020 52nd North American Power Symposium, NAPS 2020*, Apr. 2021, pp. 1–6, doi: 10.1109/NAPS50074.2021.9449758.
- [14] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, "Cybersecurity of smart electric vehicle charging: a power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020, doi: 10.1109/ACCESS.2020.3041074.
- [15] D. L. Marino *et al.*, "Cyber and physical anomaly detection in smart-grids," in *Proceedings - 2019 Resilience Week, RWS 2019*, Nov. 2019, pp. 187–193, doi: 10.1109/RWS47064.2019.8972003.
- [16] S. Kim, K. J. Park, and C. Lu, "A survey on network security for cyber-physical systems: from threats to resilient design," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 3, pp. 1534–1573, 2022, doi: 10.1109/COMST.2022.3187531.
- [17] D. Lohrmann and S. Tan, "Turning cyber incident lemons into organizational lemonade," in *Cyber Mayday and the Day After: A Leader's Guide to Preparing, Managing, and Recovering from Inevitable Business Disruptions*, 2022, pp. 169–191.
- [18] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A survey on cyber-physical systems security," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21670–21686, Dec. 2023, doi: 10.1109/IJOT.2023.3289625.
- [19] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings - Design Automation Conference*, Jun. 2010, pp. 731–736, doi: 10.1145/1837274.1837461.
- [20] A. Jones, Z. Kong, and C. Belta, "Anomaly detection in cyber-physical systems: a formal methods approach," in *Proceedings of the IEEE Conference on Decision and Control*, Dec. 2014, vol. 2015-February, no. February, pp. 848–853, doi: 10.1109/CDC.2014.7039487.
- [21] S. Guarino, F. Vitale, F. Flammini, L. Faramondi, N. Mazzocca, and R. Setola, "A two-level fusion framework for cyber-physical anomaly detection," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 1–13, 2023, doi: 10.1109/ticps.2023.3336608.
- [22] V. Cobilean, H. S. Mavikumbure, C. S. Wickramasinghe, D. L. Marino, and M. Manic, "Informed deep learning for anomaly detection in cyber-physical systems," in *Proceedings of the IEEE International Conference on Industrial Technology*, Apr. 2023, vol. 2023-April, pp. 1–7, doi: 10.1109/ICIT58465.2023.10143126.
- [23] G. Settanni, F. Skopik, A. Karaj, M. Wurzenberger, and R. Fiedler, "Protecting cyber physical production systems using anomaly detection to enable self-adaptation," in *Proceedings - 2018 IEEE Industrial Cyber-Physical Systems, ICPS 2018*, May 2018, pp. 173–180, doi: 10.1109/ICPHYS.2018.8387655.
- [24] W. Marfo, D. K. Tosh, and S. V. Moore, "Condition monitoring and anomaly detection in cyber-physical systems," in *2022 17th Annual System of Systems Engineering Conference, SOSE 2022*, Jun. 2022, pp. 106–111, doi: 10.1109/SOSE55472.2022.9812638.
- [25] Y. Raj, B. Agrawal, and M. Kirar, "A review on components of electric vehicle and Indian scenario of electric vehicles," in *2023 IEEE Renewable Energy and Sustainable E-Mobility Conference, RESEM 2023*, May 2023, pp. 1–7, doi: 10.1109/RESEM57584.2023.10236052.
- [26] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: threats and potential solutions," *Computer Networks*, vol. 169, 2020, doi: 10.1016/j.comnet.2019.107094.
- [27] S. Colabianchi, F. Costantino, G. Di Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Computers and Industrial Engineering*, vol. 160, p. 107534, Oct. 2021, doi: 10.1016/j.cie.2021.107534.
- [28] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O'Malley, and J. Barnett, "On vulnerability and resilience of cyber-physical power systems: a review," *IEEE Systems Journal*, vol. 16, no. 2, pp. 2367–2378, Jun. 2022, doi: 10.1109/JSYST.2021.3123904.
- [29] Y. Jiang, S. Wu, R. Ma, M. Liu, H. Luo, and O. Kaynak, "Monitoring and defense of industrial cyber-physical systems under typical attacks: from a systems and control perspective," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 192–207, 2023, doi: 10.1109/ticps.2023.3317237.
- [30] S. B. Weber, S. Stein, M. Pilgermann, and T. Schrader, "Attack detection for medical cyber-physical systems-a systematic literature review," *IEEE Access*, vol. 11, pp. 41796–41815, 2023, doi: 10.1109/ACCESS.2023.3270225.
- [31] S. R. Salkuti, "A survey of big data and machine learning," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 575–580, Feb. 2020, doi: 10.11591/ijece.v10i1.pp575-580.
- [32] K. Badapanda, D. P. Mishra, and S. R. Salkuti, "Agriculture data visualization and analysis using data mining techniques: application of unsupervised machine learning," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 20, no. 1, pp. 98–108, Feb. 2022, doi: 10.12928/TELKOMNIKA.v20i1.18938.
- [33] D. P. Mishra, S. Mishra, S. Jena, and S. R. Salkuti, "Image classification using machine learning," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 31, no. 3, pp. 1551–1558, Sep. 2023, doi: 10.11591/ijeecs.v31.i3.pp1551-1558.

BIOGRAPHIES OF AUTHORS






Debani Prasad Mishra     currently serves as an assistant professor and the head of the Electrical Engineering Department at the International Institute of Information Technology Bhubaneswar, Odisha. He completed his bachelor's degree in electrical engineering from Biju Patnaik University of Technology, Odisha in 2006, followed by a master's degree in power systems from IIT Delhi, India in 2010. In 2019, he successfully obtained his Ph.D. in power systems from Veer Surendra Sai University of Technology, Odisha, India. With a profound academic background and extensive knowledge of power systems, he actively engages in teaching and research activities. He is deeply passionate about sharing his expertise and guiding aspiring students in the captivating field of electrical engineering. He can be contacted at email: debani@iiit-bh.ac.in.






Rakesh Kumar Lenka    is working as an associate professor in the Department of Computer Science, Central University of Odisha. He has published over 60 research articles in reputed journals and conference proceedings. His research interests include green IoT, fog/mist computing, model checking, blockchain technology, recommendation systems, geographical information systems, and DFA-based pattern matching. He is a professional member of the CSI and the International Association of Engineers (IAENG). He has served as a reviewer for various reputed international journals and conferences. He can be contacted at email: rklenka@cuo.ac.in.






Rampa Sri Sai Yagyna Duthsharma    is currently pursuing a B.Tech. degree in electrical and electronics engineering at International Institute of Information Technology, Bhubaneswar, Odisha, India (batch 2021-2025). His interesting domains are cyber security, smart grids in EV, power electronics, and artificial intelligence. He can be contacted at email: b321064@iiit-bh.ac.in.






Pavan Kumar    is currently pursuing a B.Tech. degree in electrical and electronics engineering at International Institute of Information Technology, Bhubaneswar, Odisha, India (batch 2021-2025). His interesting domains are web development, artificial intelligence, cyber security, smart grids in EV, power electronics, electric drives, and electric vehicles. He can be contacted at email: b321055@iiit-bh.ac.in.



Lakshay Bhardwaj    is currently pursuing a B.Tech. degree in electrical and electronics engineering at International Institute of Information Technology, Bhubaneswar, Odisha, India (batch 2021-2025). His areas of interest are web development, artificial intelligence, power electronics, cyber security, smart grids in EVs, and advancements in EV battery technology exploration. He can be contacted at email: b321061@iiit-bh.ac.in.



Surender Reddy Salkuti    received Ph.D. degree in electrical engineering from the Indian Institute of Technology, New Delhi, India, in 2013. He was a postdoctoral researcher at Howard University, Washington, DC, USA, from 2013 to 2014. He is currently an associate professor at the Department of Railroad and Electrical Engineering, Woosong University, Daejeon, Republic of Korea. His current research interests include market clearing, including renewable energy sources, demand response, and smart grid development with the integration of wind and solar photovoltaic energy sources. He can be contacted at email: surender@wsu.ac.kr.