IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15489

Security Issues in Electric Vehicle Charging Infrastructure

Ms. Disha S. Gopatwar[1], Mr. Kshitij P. Tajne[2], Mr. Piyush S. Borkhade[3], Prof. A. A. Gophane[4]

Student, Department of Electrical Engineering,

Jawaharlal Darda Institute of Engineering and Technology Yavatmal, Maharashtra, India[1-3]

Assistant Professor, Department of Electrical Engineering,

Jawaharlal Darda Institute of Engineering and Technology Yavatmal, Maharashtra, India[4]

Abstract: This paper presents a comprehensive study on security issues in Electric Vehicle Charging Infrastructure (EVCI). With the rapid growth of electric vehicle adoption, charging stations have evolved into interconnected cyber-physical systems integrating communication networks, cloud platforms, and smart grid technologies [1], [9]. While these advancements enable smart charging, remote monitoring, and vehicle-to-grid (V2G) services, they also introduce significant cybersecurity risks [11], [13]. Vulnerabilities in communication protocols, firmware, authentication mechanisms, and backend management systems expose charging infrastructure to threats such as false data injection, denial-of-service attacks, malware intrusion, and unauthorized access [3], [10], [24]. These attacks can compromise user privacy, disrupt charging operations, and destabilize the power grid [2], [12]. This paper analyzes potential attack vectors and discusses security measures to enhance the resilience and reliability of EV charging systems.

Keywords: Electric Vehicle Charging Infrastructure, Cybersecurity, Smart Grid, Vehicle-to-Grid.

I. INTRODUCTION

Electric Vehicles (EVs) are rapidly transforming the transportation sector as governments and industries move toward sustainable energy solutions [9]. The increasing adoption of EVs has created strong demand for reliable and scalable Electric Vehicle Charging Infrastructure (EVCI). Modern charging stations function as cyber-physical systems integrating embedded controllers, communication networks, cloud platforms, and smart grid technologies [1], [22]. These systems enable intelligent features such as remote monitoring, authentication, billing management, smart charging, and V2G services [8], [17].

However, the integration of communication technologies introduces significant cybersecurity challenges [11], [13]. EV charging stations rely on networked protocols such as OCPP and ISO 15118 for data exchange and energy management [17], [18]. This interconnected architecture expands the attack surface and exposes the infrastructure to threats such as malware, false data injection, denial-of-service attacks, spoofing, and unauthorized access [3], [10], [24]. Exploitation of these vulnerabilities may result in financial fraud, privacy breaches, and grid instability [2], [12].

Ensuring security and resilience is therefore critical for sustainable electric mobility. Robust encryption, secure authentication, and intrusion detection mechanisms are essential to mitigate emerging threats [14], [19], [20]. A systematic analysis of vulnerabilities and countermeasures is required to strengthen EV charging ecosystems.

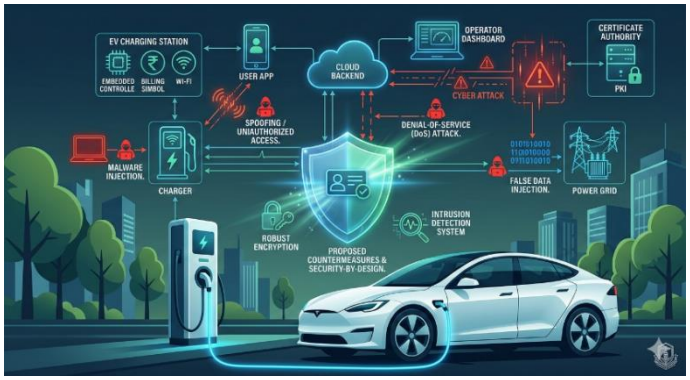

Figure 1: Architecture of Secure Ev Charging System

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15489

II. PROPOSED SYSTEM

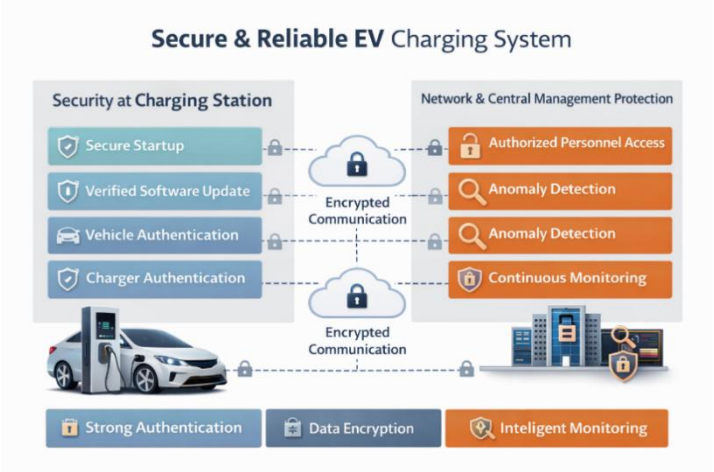

Figure 2: proposed system of Secure Ev Charging Infrastructure

The proposed system enhances EV charging security through multi-layer protection. Secure boot processes and firmware verification prevent unauthorized software modification [10], [19]. Mutual authentication using Public Key Infrastructure (PKI) ensures that only legitimate EVs and charging stations communicate [12], [17]. All communications are encrypted to protect sensitive user and payment data [11], [25].

At the network level, intrusion detection systems (IDS) and firewalls monitor abnormal activities and restrict unauthorized access [14], [22]. Network segmentation reduces the impact of compromised components. By combining authentication, encryption, and monitoring, the system ensures operational reliability and grid safety [2], [24].

III. THREAT LANDSCAPE IN EV CHARGING INFRASTRUCTURE

3.1 Cybersecurity Threats

EV charging systems face malware and ransomware threats that can disrupt operations and compromise data [10], [16]. Distributed Denial-of-Service (DDoS) attacks can overload backend servers, causing service outages [11]. Firmware manipulation may disable safety mechanisms or create persistent backdoors [19].

3.2 Network-Based Attacks

Network-based attacks include Man-in-the-Middle (MITM) attacks, spoofing, session hijacking, and replay attacks [3], [13]. These attacks exploit weak authentication and unencrypted communication channels [18].

3.3 *Physical Attacks*

Physical threats include hardware tampering, port manipulation, and side-channel attacks [21]. Such attacks can extract sensitive information or disrupt charging operations [22].

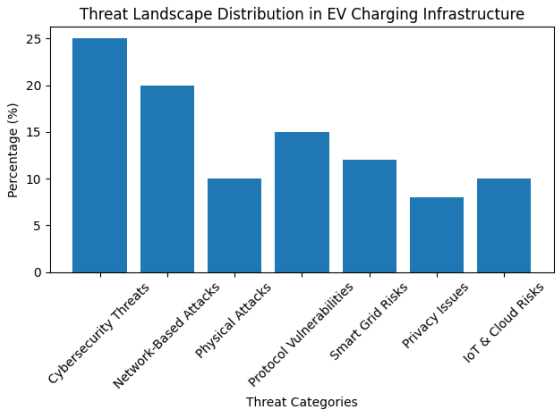

Figure 3 : graphical representation of threats

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15489

IV. VULNERABILITIES IN COMMUNICATION PROTOCOLS

Weaknesses in OCPP implementation and improper configuration can expose systems to cyberattacks [18]. Security gaps in ISO 15118 (Plug & Charge) may arise due to poor certificate management [17]. Legacy systems lacking encryption increase the risk of interception [11]. Improper certificate lifecycle management weakens trust mechanisms [12].

V. SMART GRID INTEGRATION AND GRID-LEVEL RISKS

Compromised charging stations may affect grid stability through load manipulation and coordinated attacks [2], [24]. False data injection can mislead grid operators and disrupt state estimation processes [3]. Coordinated charging attacks may overload transformers and destabilize distribution networks [8].

VI. PRIVACY ISSUES IN EV CHARGING

EV charging systems process sensitive personal and payment data [25]. Unauthorized access may expose user identities and travel patterns [12], [13]. Large-scale data aggregation may enable user profiling and misuse of personal information [16].

VII. IOT AND CLOUD SECURITY CHALLENGES

Cloud backend vulnerabilities and insecure APIs increase exposure to cyber threats [16]. Insecure firmware updates and weak authentication mechanisms further increase risk [10], [19]. Secure IoT frameworks are essential for protecting distributed charging networks [22].

VIII. ATTACK SCENARIOS AND CASE STUDIES

Real-world incidents demonstrate ransomware attacks and insecure management interfaces targeting charging operators [10], [16]. Attack models such as MITM and false data injection illustrate potential exploitation paths [3], [24]. Simulation-based assessments help evaluate resilience and improve mitigation strategies [22].

IX. SECURITY SOLUTIONS

Multi-layered security mechanisms improve resilience of EV charging systems [19], [20].

9.1 Cryptographic Solutions

End-to-end encryption protects data confidentiality [11]. PKI ensures mutual authentication [12], [17]. Secure boot and firmware signing prevent unauthorized code execution [19].

9.2 Network Security Measures

Intrusion Detection Systems detect anomalies in charging behavior [14]. Firewalls and network segmentation limit attack spread [22]. Secure APIs and encrypted channels strengthen remote management [16].

X. FUTURE RESEARCH DIRECTIONS

Future research should focus on developing quantum-resistant cryptography to protect EV charging systems from potential threats posed by quantum computing. Lightweight post-quantum algorithms suitable for embedded charging devices will be essential for long-term security[20].

With the adoption of 5G and Vehicle-to-Grid (V2G) technologies, new security challenges will emerge. Research is needed to secure high-speed communication, protect bidirectional energy exchange, and prevent grid manipulation attacks. Ensuring safe and reliable V2G integration is critical for grid stability[8],[17].

Additionally, implementing a zero-trust architecture in EV charging networks can enhance security by enforcing continuous authentication, strict access control, and network segmentation. This approach reduces the risk of insider threats and limits the impact of compromised devices[19].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.15489

XI. APPLICATIONS

- Public Charging Networks**:** Secure operation of urban, highway, and commercial charging stations with safe authentication and accurate billing.
- Residential and Workplace Charging: Protection of home and office chargers from unauthorized access, data breaches, and cyberattacks[8]
- Smart Grid Integration: Secure load management, demand response, and peak load balancing without compromising grid stability.
- Vehicle-to-Grid (V2G) Systems: Safe bidirectional energy transfer between EVs and the power grid to support renewable energy integration[9].
- Fleet Management: Secure monitoring and centralized control of electric fleets used in logistics, public transport, and corporate sectors.
- Smart City Infrastructure: Integration with IoT platforms, cloud systems, and digital payment gateways while ensuring data privacy and cybersecurity[22].

XII. CONCLUSION

The growth of electric vehicles has increased the importance of secure and reliable charging infrastructure. However, the integration of communication networks, cloud platforms, and smart grid technologies has introduced various cybersecurity and privacy risks. Vulnerabilities in protocols, backend systems, and device-level components can lead to data breaches, service disruption, and grid instability[1],[9].

By implementing strong cryptographic methods, network security measures, and intelligent monitoring systems, these risks can be minimized. A secure and resilient charging infrastructure is essential to support the sustainable and safe expansion of electric mobility in the future[14],[19],[20].

REFERENCES

[1]. S. Bayhan, G. K. Kurt, and A. Zappone, “Cyber-physical security of electric vehicle charging infrastructure,” IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2341–2375, 2021.
[2]. A. Hahn and M. Govindarasu, “Cyber attack exposure evaluation framework for the smart grid,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 835–843, 2011.
[3]. Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security, vol. 14, no. 1, pp. 1–33, 2011.
[4]. M. Erol-Kantarci and H. T. Mouftah, “Energy-efficient information and communication infrastructures in the smart grid,” IEEE Communications Magazine, vol. 49, no. 11, pp. 124–131, 2011.
[5]. N. Saputro, K. Akkaya, and S. Uludag, “A survey of routing protocols for smart grid communications,” Computer Networks, vol. 56, no. 11, pp. 2742–2771, 2012.
[6]. A. S. Musleh, G. Yao, and S. M. Muyeen, “Blockchain applications in smart grid–review and frameworks,” IEEE Access, vol. 7, pp. 86746–86757, 2019.
[7]. F. Knirsch, A. Unterweger, and D. Engel, “Privacy-preserving blockchain-based electric vehicle charging,” Computer Science–Research and Development, vol. 33, no. 1–2, pp. 71–79, 2018.
[8]. S. Rahman, M. Pipattanasomporn, and Y. Teklu, “Intelligent demand response for EV charging,” IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1273–1283, 2015.
[9]. M. Yilmaz and P. T. Krein, “Review of charging power levels and infrastructure for plug-in electric vehicles,” IEEE Transactions on Power Electronics, vol. 28, no. 5, pp. 2151–2169, 2013.
[10]. A. Paudel, T. Das, and M. A. Hossain, “Cybersecurity challenges in EV charging infrastructure,” IEEE Access, vol. 8, pp. 214578–214590, 2020.
[11]. S. Tan, D. De, W. Song, J. Yang, and S. K. Das, “Survey of security advances in smart grid,” IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 397–422, 2017.
[12]. R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “EPPA: Efficient privacy-preserving aggregation scheme for smart grid,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621–1631, 2012.
[13]. J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber security and privacy issues in smart grids,” IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981–997, 2012.
[14]. H. Sedjelmaci and S. M. Senouci, “Intrusion detection framework for EV charging,” IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2329–2338, 2017.
[15]. A. Y. S. Lam, Y.-W. Leung, and X. Chu, “Electric vehicle charging station placement,” IEEE SmartGridComm, pp. 510–515, 2013.

DOI: 10.17148/IJARCCE.2026.15489

[16]. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics," Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.
[17]. ISO 15118-2, "Road vehicles — Vehicle to grid communication interface," International Organization for Standardization, 2014.
[18]. Open Charge Alliance, "Open Charge Point Protocol (OCPP) Specification," 2020.
[19]. IEC 62443, "Industrial communication networks – Network and system security," International Electrotechnical Commission, 2018.
[20]. NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2018.
[21]. S. B. Lee and K. G. Shin, "Vulnerability assessment of EV charging stations," in Proc. IEEE PES General Meeting, 2019, pp. 1–5.
[22]. M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 446–464, 2017.
[23]. A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in Proc. 3rd USENIX Workshop on HotSec, 2008.
[24]. Y. Mo, T. H. Kim, K. Brancik, et al., "Cyber–physical security of power systems," IEEE Control Systems Magazine, vol. 32, no. 5, pp. 40–60, 2012.
[25]. D. He, S. Chan, and M. Guizani, "User privacy and data trustworthiness in smart grid communications," IEEE Wireless Communications, vol. 19, no. 3, pp. 84–89, 2012.

