IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

Wireless Power Transfer and IoT Integration for Electric Vehicle Charging: A Critical Review of Technologies, Safety, Cybersecurity and Research Gaps

Akshay Pachorkar[1], Omkar Tajanpure[2], Sahil Shaikh[3], Dr. Rahul Agarwal[4], Mrs. Sonali Gosavi[5]
Student, Department of Electrical Engineering[1-3]
Assistant Professor, Department of Electrical Engineering[4-5]
Guru Gobind Singh College of Engineering and Research Centre, Nashik, Maharashtra, India.

Abstract: *Wireless electric vehicle charging removes the plug from the charging process and, when combined with Internet of Things connectivity, promises automated, grid-aware and user-friendly charging. Research on the two subjects has, however, grown largely in parallel. This paper reviews ten recent and foundational studies drawn from IEEE, Elsevier and MDPI journals and from conference proceedings, using a recent topical review in IEEE Access as the starting point. The studies are grouped into three themes: wireless power transfer technology and roadway deployment, exposure safety and standards, and IoT communication and cybersecurity. They are compared in terms of scope, type of evidence and stated limitations, and the reported performance ranges of the main power transfer techniques are examined. The synthesis shows that inductive and resonant systems dominate practical deployment, that safety work has concentrated on field exposure limits and foreign object detection, and that cybersecurity analyses have mostly addressed conductive chargers and their back end protocols. Little work examines how communication faults or attacks interact with the power electronics of a wireless charger. Seven research gaps are identified, including cross layer threat models, field validation under realistic misalignment, common evaluation practice and harmonised standards, and a staged agenda for future work is proposed.*

Keywords: Wireless power transfer, Electric vehicles, Internet of Things, Dynamic wireless charging, Cybersecurity, Electromagnetic safety, Foreign object detection, Literature review

I. INTRODUCTION

Electric vehicle (EV) adoption has made charging infrastructure as important as the vehicles themselves [1]. Conventional plug-in chargers work well for many users, but they depend on cables, connectors and manual handling, which wear out, are exposed to weather and can be awkward for some drivers. Wireless electric vehicle charging (WEVC) avoids these issues by moving energy across an air gap with magnetic or electric fields. It can be applied to parked vehicles, to vehicles waiting at stops, and to vehicles in motion on instrumented roads [2], [3].

At the same time, charging is becoming a networked service. Chargers report their status to back end platforms, receive scheduling and pricing commands, and exchange authorisation data with vehicles. For a wireless charger, Internet of Things (IoT) technologies can in principle add coil position sensing, foreign object monitoring, segment switching on a roadway and billing, all coordinated through communication links. The same links, however, widen the attack surface. Studies of conductive charging have already shown that weaknesses in charge point protocols, charger firmware and vendor back ends can be exploited [4]–[6]. A wireless charger inherits these exposures and adds high power resonant hardware whose misbehaviour has physical safety consequences.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-40144

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, October 2026 Impact Factor: 8.2

A recent topical review in IEEE Access [1] brings these strands together. It classifies the main wireless power transfer (WPT) techniques, discusses implementation challenges, health and safety, policy and standards, and treats IoT and cybersecurity as a system level dimension. The present paper uses that work as its starting point but does not restate it. Instead, it examines ten independent studies, compares what each of them actually contributes, and asks what is still missing when the studies are read together.

1.1 Scope and Review Method

The search was carried out in October 2026. Candidate papers were located through web searches that surface publisher pages, indexing services and institutional repositories, using combinations of the terms wireless EV charging, roadway powered electric vehicles, foreign object detection, electromagnetic field exposure, OCPP security and EV charging cybersecurity. A study was retained when it was peer reviewed or presented at a recognised conference, dealt directly with wireless charging or with the communication and security of EV charging, and gave enough information to be compared with the others. The title, authors, venue, volume, pages and DOI of every retained record were cross-checked against the publisher page, an indexing record or an institutional repository entry.

Ten studies were selected to cover three themes rather than to exhaust the literature, so this is a critical narrative review and not a formal systematic review. The ICNIRP exposure guideline [7] is cited as a normative document and is not counted among the ten. Numerical values quoted from the studies are reported as the original authors give them and were not recomputed.

1.2 Contributions of This Review

The contributions are fourfold. First, the ten studies are summarised in a common format (Table 2). Second, they are compared across scope, type of evidence and publication period. Third, a layered view of a WPT and IoT charging system is proposed to show where each study sits and which interfaces remain unexamined (Fig. 1). Fourth, seven research gaps are identified and translated into a staged agenda for future work.

II. BACKGROUND: WIRELESS EV CHARGING AND IOT

2.1 Operating Principle

A wireless charger is built around two magnetically coupled coils. A high frequency inverter drives the transmitter coil, which is buried in a ground pad or road surface. The receiver coil under the vehicle floor picks up the alternating flux, and a rectifier and converter condition the power for the battery. Because the coils are loosely coupled, a large share of the apparent power is reactive, so capacitors or capacitor and inductor networks are added on both sides to bring the circuit to resonance. Series-series, series-parallel and LCC arrangements are the usual choices, and each trades output behaviour, tolerance to load change and sensitivity to coil separation differently [1]. Coil design, compensation topologies, power converters and control are consistently identified as the core technical elements of the field [2].

Transferred power and efficiency therefore depend on the coupling coefficient, which falls with air gap and lateral offset, and on how closely the operating frequency tracks the resonant frequency. This sensitivity to alignment is one reason why coil structure, adaptive control and, on roads, segmented transmitters have received so much attention [3].

2.2 Comparison of WPT Techniques

Table 1 and Chart 1 reproduce the indicative ranges compiled in the base review [1] for five families of techniques. These figures aggregate results from different sources, test conditions and power levels, so they are read here as typical ranges and not as measured, like for like performance.

Table -1: Indicative characteristics of WPT techniques, as compiled in [1]

Technique	Power	Efficiency	Maturity
Inductive (IPT)	3.3–22 kW	85–93 %	Commercial, standardised
Resonant inductive	3.3–50 kW	88–95 %	Pilot scale, pre-commercial

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

Technique	Power	Efficiency	Maturity
Capacitive (CPT)	1–7 kW	70–85 %	Experimental, early prototype
Microwave / RF	mW–100 W	below 50 %	Research stage
Hybrid	7–22 kW	80–92 %	Experimental, pilot scale

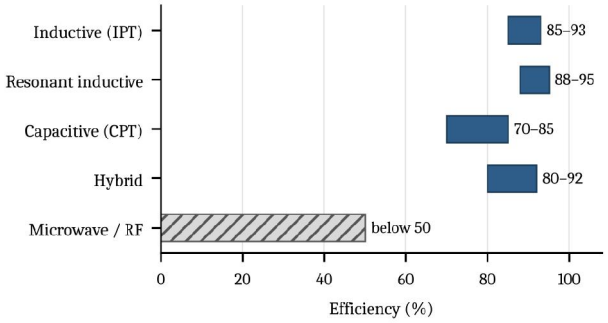


Chart -1: Indicative efficiency ranges of WPT techniques as compiled in [1]

Two patterns stand out. Inductive and resonant systems combine the highest efficiency with the highest power and the greatest technological maturity, which explains why the studies reviewed in Section 3 concentrate on them. Capacitive and microwave approaches remain confined to low power or niche uses, and hybrid designs sit in between and are mostly at pilot stage.

2.3 A Layered View of IoT-Enabled Wireless Charging

For the purpose of this review, an IoT-enabled wireless charger is described by four elements (Fig. 1). The physical WPT layer contains the coils, compensation network, power converters and protective sensing. The communication and control layer carries sensor data, vehicle to charger messaging and back end commands.

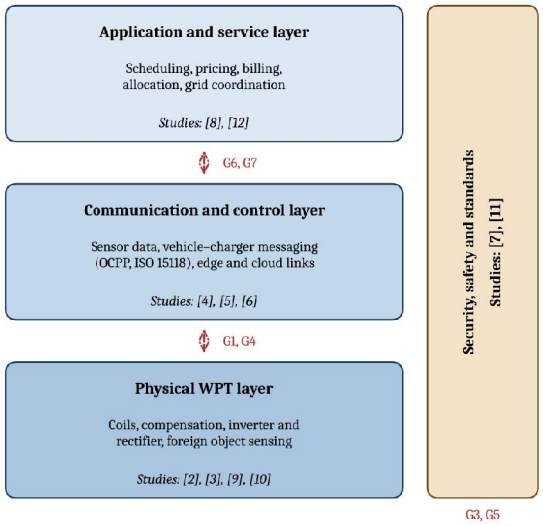


Fig -1: Layered view of a WPT and IoT charging system. Reference numbers show the layer each reviewed study mainly addresses; dashed links mark interfaces that remain largely unexamined (G1 to G7, Section 5)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

The application and service layer handles scheduling, pricing, billing, user interaction and grid coordination. Security, safety and standards act across all three. A similar three layer decomposition is used in the base review [1]. The version used here adds the cross cutting column and is used to position the studies in Section 3 by the layer they mainly address. The mapping is the authors' own reading of each study's stated scope and is not a classification given by the original papers.

III. REVIEW OF SELECTED STUDIES

Table 2 lists the ten studies by theme. The subsections that follow discuss each one and add a short critical comment on what it does and does not cover.

Table -2: Summary of the ten reviewed studies

Ref.	Theme, type, year	Main contribution
[2]	WPT technology; review; 2016	Coil, compensation, converter and control overview with deployments and sustainability assessment
[3]	Roadway WPT; review; 2016	OLEV generations; coil structures, power supply schemes and segmentation switching
[8]	Operations and systems; survey; 2018	Infrastructure allocation, cost-benefit analysis, billing and pricing for wireless charging EVs
[9]	EMF safety; review; 2020	Exposure limits, shielding, compiled field measurements, living and foreign object detection
[10]	Foreign object detection; review; 2026	Taxonomy of metal and living object detection with comparison and finite element analysis
[11]	Standards; survey; 2019	IEC, ISO and SAE documents, ICNIRP limits and medical device immunity
[4]	Protocol security; analysis with simulation; 2017	OCPP threats, with denial of service and fraud shown in a simulator
[5]	Grid cybersecurity; review; 2020	Backdoors across EVs, chargers and grid; effects of coordinated manipulation
[6]	Charger cybersecurity; review; 2022	Disclosed vulnerabilities, impacts and defences across device, communication and cloud
[12]	Grid integration and Internet of Energy; review; 2025	Charging technologies and data dissemination; agent based modelling for renewables

3.1 Technology and Deployment Studies

Bi et al. [2] give a broad account of WPT for EVs. They cover coil design, compensation topologies, power electronic converters and control methods, record real world deployments, and extend the discussion to energy, environmental and economic performance, policy drivers, and health and safety. Its strength is that it links engineering choices to sustainability outcomes. As a 2016 paper it predates the current wave of IoT based charging services, and the communication layer is not among the topics listed in its abstract, so it cannot be used on its own to judge how connectivity affects a wireless charger.

Mi et al. [3] concentrate on roadway powered electric vehicles and contrast them with stationary charging. They explain how better semiconductor switches, coil design, road construction methods and higher operating frequencies have raised power capacity and efficiency while improving lateral tolerance, air gap, field levels, size, weight and cost. The discussion centres on the fifth and sixth generations of the online electric vehicle (OLEV) systems and closes with technical issues of lumped inductive systems: coil structures, power supply schemes and segmentation switching.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

Segmentation switching is the point at which a roadway system needs timely knowledge of vehicle position, which makes it a natural entry point for sensing and communication, although the study frames it mainly as a power electronics issue.

Jang [8] takes a systems and operations view. The survey introduces terminology and past and current implementations of wireless charging EVs, and then reviews work on infrastructure allocation, cost-benefit analysis, billing and pricing, and supporting facilities before proposing future research directions. It is valuable because it shows that planning and economic questions are as decisive for deployment as coil efficiency. Its stated scope does not extend to the communication and security requirements that billing and monitoring would impose.

3.2 Safety, Exposure and Standards

Asa et al. [9] review exposure limits for the intermediate frequency fields emitted by WEVC systems. They summarise limits from international guidelines, compare shielding technologies in terms of geometry, materials and performance, collect laboratory field measurements from several WPT studies at different power levels, and discuss field reduction practice with case studies from Oak Ridge National Laboratory. Living object and foreign object detection are examined from a safety point of view. The paper is useful because it places exposure limits and measured data side by side. Because the measurements come from studies with different coil designs and power levels, they demonstrate feasibility rather than provide a basis for a general compliance statement.

The ICNIRP guideline [7], which underlies most exposure assessments, sets basic restrictions on the electric field induced inside the body to protect against effects on the nervous system, and derives external reference levels for electric field, magnetic field and contact current. Exceeding a reference level does not by itself mean that a basic restriction is exceeded, so a further assessment is then needed. Two points matter for wireless charging. Compliance with the basic restriction is judged on a small averaging volume of tissue, which makes it dependent on detailed coil and body modelling. In addition, the stated range of the guideline ends at 100 kHz, whereas the base review [1] reports inductive charging operation up to the order of 150 kHz, so systems near the upper end of that range need to be assessed against guidance that covers higher frequencies.

Grazian et al. [11] survey the standards and regulations that apply to wireless charging, including IEC 61980-1, ISO/PAS 19363:2017, SAE J2954, the ICNIRP 2010 limits for the general public and Annex M of AAMI/ISO 14117 on implantable medical devices such as pacemakers. The survey makes clear that interoperability, exposure and medical device immunity are covered by different documents issued by different bodies. The documents named in its record are concerned with power transfer, interoperability and exposure, and communication security is not highlighted among them, suggesting that cybersecurity is not yet built into the wireless charging standards.

Alam et al. [10] offer the most recent review in this group, devoted to foreign object detection (FOD) in inductive WPT. Methods are divided into metal object detection and living object detection and classified by sensing principle: electrical parameter monitoring, magnetic field sensing, thermal, capacitive, ultrasonic, vision based and hybrid approaches. They are compared on accuracy, cost, robustness to the environment and real time suitability. The paper also reports finite element analysis of how cast iron, steel, aluminium and water change coil parameters and efficiency, and it names artificial intelligence driven sensor fusion and standardised validation platforms as open needs. Sensor fusion implies data movement between detectors, controllers and possibly remote services, so the latency and integrity of that data become safety relevant, a point on which the abstract is silent.

3.3 IoT, Communication and Cybersecurity

Alcaraz et al. [4] examine the Open Charge Point Protocol (OCPP), which links charge points to central management systems. They find that OCPP relies on lower layer protection, leaves commissioning and session bootstrapping unspecified, and assumes trustworthy components. The threats they identify include impersonation of a charge point, manipulation of start-up and configuration messages, tampering with charging profiles, meter fraud and energy theft, and abuse of reservation and offline modes. Using an OCPP simulator with network attack tools, they demonstrate a

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, October 2026 Impact Factor: 8.2

heartbeat based denial of service and a fraud scenario, and they recommend secure channels, lightweight intrusion detection, strong authentication, detailed logging and adherence to IEC 62351. It is the clearest threat analysis of a charging management protocol in this set. It remains a simulation based demonstration on charge points in general, and whether wireless pads add protocol level exposures is not addressed.

Acharya et al. [5] look at the same problem from the power grid side. They catalogue known and potential backdoors across vehicles, charging stations and the grid, cite publicly reported flaws in commercial charger products, and note that the EV internal network, the charger to vehicle interface and station software are all weak points. In their assessment, ISO 15118 lacks robust message authentication and encryption. Drawing on cited studies, they show how coordinated manipulation of many chargers could shift demand enough to trigger frequency or voltage events, with a Manhattan example in which about 1,000 EVs charging at 350 kW could be sufficient to trip over-frequency relays. They call for standardised protocols with built-in security, protection of legacy equipment and resilience to unknown attacks. The paper is persuasive about grid level consequences, although the quantified examples come from specific network models and should not be transferred directly to other systems, and its abstract does not single out wireless chargers.

Johnson et al. [6] survey publicly disclosed vulnerabilities in EV chargers, the impact of charger cyber attacks and proposed defences. They report weaknesses in charging hardware, in its communication with vehicles and in upstream services such as vendor clouds, third party systems and grid operators, with consequences ranging from minor local effects to prolonged national disruptions, and they argue that established IT and operational technology security practice can be applied to this domain. The message that defence has to span device, communication and cloud is the closest this set comes to a system level view. The focus remains on chargers in general, so the power transfer hardware of a wireless system is outside the stated scope.

Kavousighahfarokhi et al. [12] review charging station technologies together with data dissemination under the Internet of Energy concept. Topics include charging technologies, energy transfer, batteries, charging schemes, management standards, distributed energy management, connectivity issues and neural network based optimisation. The authors report that agent based modelling enabled by the Internet of Energy can raise renewable energy utilisation by 50.1 percent. This figure is reported from the modelling studies the authors summarise, so it is best treated as an illustration of potential and not as an expected field result. The review gives the most explicit link between charging and data infrastructure in this set, but it treats charging technologies broadly and the physical behaviour of wireless power transfer is not its focus.

IV. COMPARATIVE ANALYSIS AND SYNTHESIS

4.1 Scope, Evidence and Time Span

Read side by side, the ten studies divide into three groups that rarely overlap. The technology group [2], [3], [8] deals with coils, converters, roadways and economics. The safety group [9]–[11] deals with exposure, detection and standards. The cybersecurity and IoT group [4]–[6], [12] deals with protocols, chargers and the grid. Within the scope described in their abstracts, none of the cybersecurity studies analyses a wireless charger specifically, and none of the technology studies analyses a communication attack.

The type of evidence also differs. The studies in [2], [3], [8] are narrative reviews, [9] compiles laboratory field measurements, [10] adds finite element analysis, [4] demonstrates attacks in a simulator, [5] draws on grid case studies, and [6], [12] summarise disclosed vulnerabilities and modelling results. These forms of evidence are not interchangeable, and no common metric allows, for example, the safety margin of a detection method to be compared with the risk reduction of an authentication scheme.

Publication dates run from 2016 to 2026. The technology reviews are the oldest (2016 to 2018), the cybersecurity studies span 2017 to 2025, and most of the safety material dates from 2019 onwards. The most detailed technical surveys of power transfer were therefore written before the most detailed surveys of charging cybersecurity, which may help to explain why the two have not been connected.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

4.2 Cross-Layer Interactions

Reading the studies together suggests several interactions that none of them examines directly. They are inferences by the authors of this review and not results reported in the studies.

The first concerns command integrity and field exposure. Alcaraz et al. [4] show that tampered charging profiles can drive power above or below intended limits. In a wireless charger, a power set-point is typically realised by adjusting inverter operation, which also changes the field around the vehicle and the heating of any foreign object present. A manipulated command could therefore be a safety event as well as a grid event.

The second concerns detection latency. The sensor fusion methods foreseen in [10] need data to travel between sensors and controllers, and the shutdown decision has to be taken in time. If any part of that path relies on a network that can be delayed or spoofed [6], the protection function itself becomes open to attack.

The third concerns segmented roadways and aggregate demand. Segmentation switching [3] requires continuous vehicle position information. With many vehicles, the aggregate load seen by the grid [5] depends on that information, and false position data could produce abrupt load changes. Finally, standards address exposure and interoperability [11], whereas security recommendations for EV charging are described as fragmented and not enforced [5].

4.3 Relation to the Base Review

The observations above are consistent with the research gaps listed in the base review [1]: reliance on simulation, weak integration of hardware and communication layers, and the absence of common protocols. The independent studies add two points. First, the evidence behind each gap is heterogeneous, which is why the quantitative comparisons in the base review, for instance the ranges in Table 1, have to be read as indicative. Second, the comparison figure in the base review rates earlier surveys on a 0 to 5 coverage scale. The scoring rubric is not detailed in the text, and the scores are assigned by the authors, so they summarise the authors' judgement but are not an independently reproducible measure.

V. RESEARCH GAPS

Seven gaps follow from the synthesis. Table 3 relates each of them to the evidence in the reviewed studies and to the kind of work that is needed.

Table -3: Research gaps identified from the review

ID	Gap	Evidence	Work needed
G1	Wireless specific cyber-physical threat models	Security studies address chargers, protocols and grid [4]–[6]	Threat models and testbeds that include inverter, coil and detection functions
G2	Field validation under realistic conditions	Field data compiled from separate laboratory studies [9]; reliance on simulation noted in [1]	Long duration trials with misalignment, weather and traffic
G3	No common evaluation basis	Evidence types and power levels differ (Section 4.1)	Shared benchmarks and reporting templates for power, gap, offset, field, efficiency and latency
G4	Safety functions that depend on real time data	FOD methods compared; sensor fusion and validation platforms are open needs [10]	Latency bounded, secure detection architectures; open validation platforms
G5	Standards and exposure at higher frequencies	Several documents from different bodies [11]; guideline range ends at 100 kHz [7]; security fragmented [5]	Joint treatment of transfer, exposure, interoperability and security

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-40144

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 5, October 2026 Impact Factor: 8.2

ID	Gap	Evidence	Work needed
G6	Economics and operations coupled to data	Allocation, cost-benefit and billing [8]; data dissemination [12]	Models that include communication cost, data governance and billing integrity
G7	Grid resilience of wireless charging	Coordinated manipulation of chargers [5]; Internet of Energy modelling [12]	Co-simulation of wireless load, communication and grid under attack

VI. FUTURE SCOPE

The gaps above can be addressed in stages that build on one another.

Near term. The first need is shared foundations. A minimal benchmark set for WPT and IoT studies should state power level, air gap, lateral offset, field levels, efficiency and communication latency, so that results become comparable (G3). A wireless specific threat model should list the assets that differ from conductive charging, namely inverter control, pad firmware, detection sensors and position data (G1). Open datasets of detection signals and communication traces would help both lines of work.

Medium term. Hardware in the loop testbeds that combine a resonant converter with a charging protocol stack and controlled attack injection would allow the interactions in Section 4.2 to be tested directly (G1, G2). Secure and time bounded communication for segment switching and for detection should be designed and evaluated together with the power stage (G4). Detection methods based on sensor fusion need explicit latency and false alarm budgets. Economic models should include communication, data handling and billing integrity (G6).

Long term. Standards bodies could treat power transfer, exposure, interoperability and cybersecurity as one conformity problem, including guidance for operation above 100 kHz (G5). Field pilots in controlled settings such as bus lanes or logistics corridors should run long enough to capture ageing, weather and traffic effects (G2). As bidirectional charging spreads, co-simulation of wireless charging, communication and grid operation under attack will be needed to judge resilience (G7). Privacy preserving techniques such as federated learning, which the base review [1] mentions for charging data, should be assessed in the same framework.

VII. CONCLUSIONS

This review used a recent topical paper [1] as its foundation and examined ten independent studies on wireless charging technology, safety and standards, and IoT and cybersecurity. The technology literature shows that inductive and resonant systems are the most mature, and that roadway deployment depends as much on planning and economics as on coil design. The safety literature has concentrated on exposure limits, shielding and foreign object detection, while the standards landscape is spread across several bodies. The cybersecurity literature has documented real weaknesses in charging protocols, chargers and their back ends, with potential effects on the grid, but it has mostly addressed conductive charging.

The central finding is that these strands have not yet been connected. Command integrity, detection latency and position data link the communication layer to the power stage and to safety, yet no reviewed study analyses these links for a wireless charger. Closing the seven gaps identified here, beginning with common benchmarks and wireless specific threat models, would give designers, regulators and operators a firmer basis for secure, safe and scalable wireless EV charging. Because the review is narrative and limited to ten studies, its conclusions should be tested against a wider systematic search in later work.

ACKNOWLEDGEMENT

The authors thank their project guide and department for guidance and support during the preparation of this review.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 5, October 2026
Impact Factor: 8.2

REFERENCES

1. S. Karim, S. T. Chauhdary, H. Kamil, F. Mumtaz, and G. Farid, "Wireless power transfer and IoT in EV charging: Opportunities, challenges, and future directions," IEEE Access, vol. 14, pp. 40672–40689, 2026, doi: 10.1109/ACCESS.2026.3668809.
2. Z. Bi, T. Kan, C. C. Mi, Y. Zhang, Z. Zhao, and G. A. Keoleian, "A review of wireless power transfer for electric vehicles: Prospects to enhance sustainable mobility," Applied Energy, vol. 179, pp. 413–425, 2016, doi: 10.1016/j.apenergy.2016.07.003.
3. C. C. Mi, G. Buja, S. Y. Choi, and C. T. Rim, "Modern advances in wireless power transfer systems for roadway powered electric vehicles," IEEE Trans. Ind. Electron., vol. 63, no. 10, pp. 6533–6545, Oct. 2016, doi: 10.1109/TIE.2016.2574993.
4. C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP protocol: Security threats and challenges," IEEE Trans. Smart Grid, vol. 8, pp. 2452–2459, 2017, doi: 10.1109/TSG.2017.2669647.
5. S. Acharya, Y. Dvorkin, H. Pandžić, 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.
6. J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," Energies, vol. 15, no. 11, Art. no. 3931, 2022, doi: 10.3390/en15113931.
7. International Commission on Non-Ionizing Radiation Protection (ICNIRP), "Guidelines for limiting exposure to time-varying electric and magnetic fields (1 Hz to 100 kHz)," Health Physics, vol. 99, no. 6, pp. 818–836, Dec. 2010, doi: 10.1097/HP.0b013e3181f06c86.
8. Y. J. Jang, "Survey of the operation and system study on wireless charging electric vehicle systems," Transp. Res. C, Emerg. Technol., vol. 95, pp. 844–866, Oct. 2018, doi: 10.1016/j.trc.2018.04.006.
9. E. Asa, M. Mohammad, O. C. Onar, J. L. Pries, V. P. Galigekere, and G.-J. Su, "Review of safety and exposure limits of electromagnetic fields (EMF) in wireless electric vehicle charging (WEVC) applications," in Proc. IEEE Transp. Electrific. Conf. Expo (ITEC), Chicago, IL, USA, Jun. 2020, pp. 17–24, doi: 10.1109/ITEC48692.2020.9161597.
10. B. Alam, S. Mekhilef, F. Khan, M. Mubin, T. K. Soon, A. Wahyudie, M. M. Hashmi, M. Seyedmahmoudian, and A. Stojcevski, "A comprehensive review of foreign object detection methods in wireless power transfer for electric vehicles with conceptual analysis," IEEE Access, vol. 14, pp. 18897–18912, 2026, doi: 10.1109/ACCESS.2025.3617934.
11. F. Grazian, W. Shi, J. Dong, P. van Duijsen, T. B. Soeiro, and P. Bauer, "Survey on standards and regulations for wireless charging of electric vehicles," in Proc. AEIT Int. Conf. Elect. Electron. Technol. Automot. (AEIT AUTOMOTIVE), Torino, Italy, 2019, pp. 1–5.
12. A Kavousighahfarokhi, M. A. Hannan, S. M. Abu, P. J. Ker, R. T. K. Wong, and G. Jang, "Grid-integrated electric vehicle charging station technologies and data dissemination through internet of energy use," Renew. Sustain. Energy Rev., vol. 220, Art. no. 115904, 2025, doi: 10.1016/j.rser.2025.115904.