IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12746

Review of Secure, Robust, and Intuitive Charging Solutions for Electric Vehicles

Parul M Vachhani[1], Shukla Darshan H[2], Rina R Prajapati[3]

Lecturer, Electrical, C U Shah Polytechnic, Surendranagar, Gujarat India[1]

Lecturer, Electrical, C U Shah Polytechnic, Surendranagar, Gujarat India[2]

Lecturer, Electrical, C U Shah Polytechnic, Surendranagar, Gujarat India[3]

Abstract: The rapid adoption of Electric Vehicles (EVs) necessitates a secure, robust, and intelligent Electric Vehicle Charging Station (EVCS) infrastructure to support sustainable transportation. While EVs offer significant environmental benefits, their supporting systems face critical cybersecurity vulnerabilities and usability challenges. This paper examines EVCS threats using the STRIDE model, evaluates existing protocols (ISO 15118, OCPP), and explores integration with smart grids and Vehicle-to-Grid (V2G) systems. It proposes a layered defence model with encryption, authentication upgrades, and advanced solutions like AI-based monitoring and blockchain. Furthermore, it emphasizes the importance of intuitive design and robust system architecture to ensure high availability, ease of use, and user trust. Unified standards, strong policy mandates, and public-private collaboration are recommended to enhance EVCS resilience and usability.

Keywords: Introduction, Threat Landscape and STRIDE Model, Key Vulnerabilities in EVCS Systems, EVCS Security Protocols and Shortcomings, Countermeasures and Best Practices, Grid Integration and Systemic Challenges, Enhancing Robustness in EVCS Infrastructure, Designing Intuitive Charging Systems, Policy, Standards, and Regulatory Frameworks, Future Directions, Conclusion

I. INTRODUCTION

The global push for decarbonization has led to a significant rise in Electric Vehicle (EV) adoption. A cornerstone of this transition is the Electric Vehicle Charging Infrastructure (EVCI), which must be secure, resilient, and user-friendly. With the proliferation of smart and connected charging stations, the attack surface has expanded, exposing users, grid operators, and service providers to cyber threats. Additionally, users demand fast, intuitive, and reliable charging experiences. Ensuring the integrity, robustness, and usability of EVCS systems is crucial to sustaining public trust and grid stability[1]

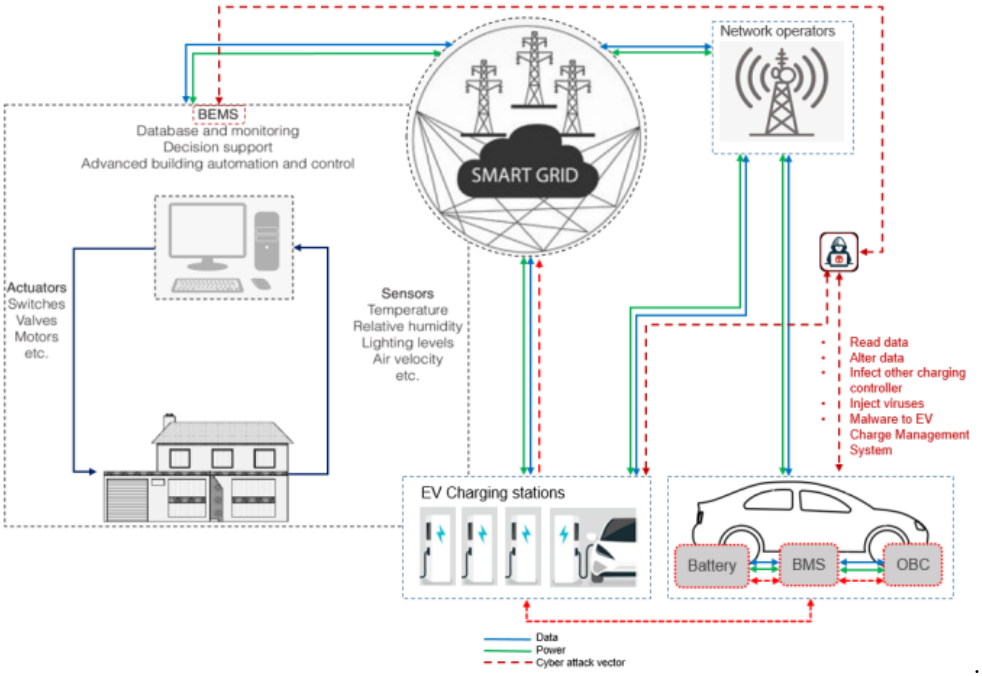


Fig 1 Smart Charging system

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12746

II. THREAT LANDSCAPE AND STRIDE MODEL

2. Threat Landscape and STRIDE Model Cybersecurity threats in EVCS systems can be systematically analysed using the STRIDE model:[1]

- Spoofing: Attackers can impersonate legitimate users or charging stations.
- Tampering: Modifying firmware or altering data on the charger.
- Repudiation: Lack of proper logs enables denial of malicious actions.
- Information Disclosure: Leakage of private user or grid data due to poor encryption.
- Denial of Service (DoS): Overloading systems to prevent charging.
- Elevation of Privilege: Exploiting vulnerabilities to gain higher access.

Real-world example: Attackers can spoof RFID-based authentication or manipulate firmware to inject malware into the grid.

III. KEY VULNERABILITIES IN EVCS SYSTEMS [2]

1. Authentication: Legacy RFID UIDs can be cloned easily, Many Electric Vehicle Charging Systems still use legacy RFID (Radio Frequency Identification) cards for user authentication. These older systems often rely solely on the card's UID (Unique Identifier) for granting access. However, these UIDs are not encrypted and can be easily read and cloned using low-cost tools, posing a significant security threat. An attacker can use a cloned card to:

   - Illegally access charging services.
   - Impersonate legitimate users.
   - Bypass billing or usage limits.

2. Protocol Flaws: Older OCPP versions (e.g., 1.5, 1.6) do not enforce TLS.
   The Open Charge Point Protocol (OCPP) is widely used for communication between EV charging stations and central management systems. However, older versions like OCPP 1.5 and 1.6 do not enforce the use of TLS (Transport Layer Security) by default. As a result:

   - Data is transmitted in plaintext, making it vulnerable to eavesdropping.
   - Attackers can perform Man-in-the-Middle (MitM) attacks to intercept, alter, or spoof messages.
   - Malicious commands can be injected to disrupt charging sessions or alter billing data.

3. Firmware: Poorly updated or unsecured firmware increases risk. Electric Vehicle Charging Stations rely on embedded firmware to control operations and enable features. However, many systems either lack secure update mechanisms or are rarely updated, leading to serious security risks

4. Physical Ports: USB or serial ports are often left unprotected. Many EV charging stations are equipped with USB, serial, or other maintenance ports for diagnostics and servicing. However, these physical interfaces are often exposed or poorly secured, creating a critical attack surface:

   - Attackers can gain direct access to the internal system via these ports.
   - It allows for firmware dumping, data theft, or even installation of malware.
   - In some cases, attackers can bypass authentication or gain administrative privileges using physical access.

5. APIs and Cloud Platforms: Weak API security on cloud platforms can expose user data. EV charging systems often connect to cloud-based platforms for management, billing, monitoring, and user services via APIs (Application Programming Interfaces). However, if these APIs are poorly secured, they become a major vulnerability:

Insufficient authentication or authorization checks can allow unauthorized access to sensitive user or system data.
APIs may be susceptible to common attacks like injection, broken access control, or rate-limiting bypass.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12746

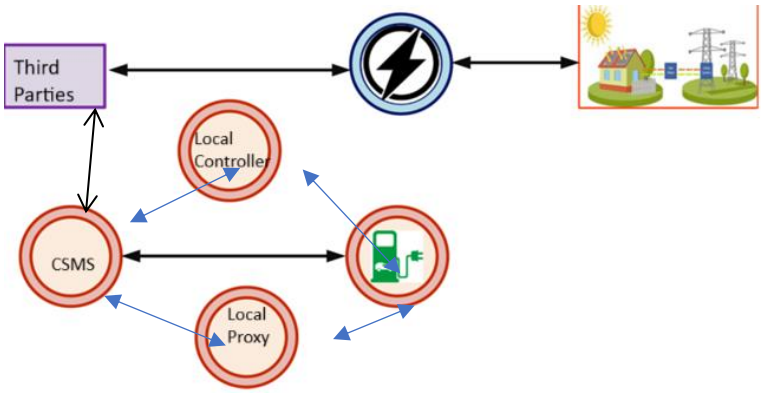


Fig 2. EV charging OCPP Framework

IV. EVCS SECURITY PROTOCOLS AND SHORTCOMINGS [4]

1. ISO 15118: Introduces Plug-and-Charge with TLS support, but PKI implementation is inconsistent ISO 15118 is a communication standard enabling Plug-and-Charge, where EVs automatically authenticate and initiate charging securely via TLS encryption. While it improves convenience and security, its effectiveness relies on Public Key Infrastructure (PKI) — and that's where vulnerabilities arise:
   - Inconsistent or incomplete PKI implementation across vendors and networks weakens trust.
   - Misconfigured or poorly managed certificates can lead to authentication failures or unauthorized access.
   - Some charging stations or vehicles may skip certificate validation, defeating the purpose of secure communication.
2. OCPP: A standard for charger-CPO communication. OCPP 2.0 improves security, but many chargers still use older insecure versions. The Open Charge Point Protocol (OCPP) is the de facto standard for communication between EV chargers and Charge Point Operators (CPOs). It enables remote control, monitoring, and management of charging stations
3. OCPI/OCHP: May lack encryption by default, increasing the risk of MITM attacks.
4. Authentication Methods: Static identifiers (e.g., RFID) are outdated; dynamic methods like EMV-based and pseudonymous credentials offer better protection.

V. COUNTERMEASURES AND BEST PRACTICES [5]

1. Technical Security Measures:
   - Enforce TLS 1.3 encryption with strong cipher suites.
   - Use FIPS 140-3 compliant cryptographic modules.
   - Implement Intrusion Detection Systems (IDS) at EVCS gateways.
   - Secure Over-the-Air (OTA) firmware updates with code signing.
   - Apply Role-Based Access Control (RBAC) for administrative access.
2. Advanced Authentication Solutions:
   - QEVSEC Protocol: Lightweight authentication for DWPT using XOR, hashing, session-specific pseudonyms.
   - Proven secure via formal verification tools like BAN logic and Scyther.
3. AI and Blockchain Integration:
   - AI can detect anomalous energy usage or login attempts.
   - Blockchain ensures data integrity and transaction traceability.
4. Digital Forensics Readiness:
   - Implement audit logging aligned with ISO/IEC 27043 for effective incident response.

VI. GRID INTEGRATION AND SYSTEMIC CHALLENGES [3]

1. Vehicle-to-Grid (V2G):
   - Bidirectional flow creates new attack vectors like voltage instability.
   - Aggregator compromise can lead to orchestrated grid attacks.
2. Power System Overload:
   - Clustering of high-power chargers may overload transformers.
   - Harmonics can degrade power quality.

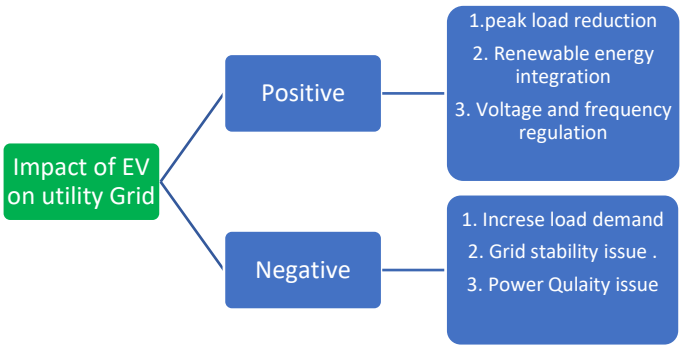
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12746

3. Smart Charging & Demand-Response:
   - Dynamic charging based on real-time grid signals improves efficiency but requires secure APIs and protocols like OpenADR



VII. ENHANCING ROBUSTNESS IN EVCS INFRASTRUCTURE [4]

- Redundancy and Failover: Implement backup systems and fail-safes to maintain uptime.
- Hardware Durability: Weatherproof, vandal-resistant enclosures extend charger lifespan.
- Power Conditioning: Use surge protectors, harmonic filters, and voltage regulators.
- Modular Architecture: Allows easy replacement of faulty components without downtime.
- Resilient Communication Links: Dual SIM, edge computing, and mesh networking enhance connectivity.

VIII. FUTURE DIRECTIONS [5]

- Offline Authentication: Secure NFC or EMV support for rural/off-grid chargers.
- Virtual Power Plants (VPPs): Aggregated EVs support the grid.
- Unified Standards: Combine IEC 62443, ISO 15118, and cybersecurity policies.
- User Training: Awareness programs for charge point operators and users.
- AI-Powered Predictive Maintenance: Prevent breakdowns using sensor data.
- Augmented Reality (AR) Diagnostics: Intuitively improve field maintenance.

IX. CONCLUSION

Electric vehicle charging stations are essential to future mobility, but their design must be secure, resilient, and intuitive. With increasing integration into power systems and smart cities, vulnerabilities and inefficiencies can have far-reaching consequences. This paper recommends a multi-layered security architecture, robust physical and digital infrastructure, and user-friendly design. Strong cryptographic protocols, dynamic authentication, AI-driven intrusion detection, and regulatory support are critical. A collaborative and user-focused approach is vital to ensuring safe, reliable, and seamless EV charging experiences.

REFERENCES

[1]. Security of Electric Vehicle Charging Stations, Sunbramaiam Ganesan Dhrumil Kamleshbhai Patel Rhea Chokhlingam Oklan University, journal of electrical and computer engineering research vol. 4, no. 4, 2024

[2]. Electric vehicle charging technologies, infrastructure expansion, grid integration strategies, and their role in promoting sustainable e-mobility, Arvind R. Singh a, Pradeep Vishnuram b,*, Sureshkumar Alagarsamy b, Mohit Bajaj c,d,e,**, Vojtech Blazek f, Issam Damaj g, Rajkumar Singh Rathore g,*, Fahd N. Al-Wesabi h,Kamal M. Othman, Elsevier

[3]. QEVSEC: Quick Electric Vehicle SEcure Charging via Dynamic Wireless Power Transfer. Tommaso Bianchi Dept. of MathematicsUniversity of PadovaPadua, Italytommaso.bianchi@phd.unipd.it

[4]. Security of EV-Charging Protocols. Pol Van Aubel1, Erik Poll1,Digital Security group, Institute for Computing and Information Sciences, Radboud University Toernooiveld 212, 6525 EC, Nijmegen, the Netherland

[5]. Cyber Security of Electric Vehicle Charging Infrastructure: Open Issues and Recommendations, Inna Skarga-Bandurova School of Engineering, Computing and Mathematics Oxford Brookes University Oxford, United Kingdom iskarga-bandurova@brookes.ac.uk ORCID ID: 0000-0003-3458-8730