Chapter 1
AI-Driven Predictive Approaches for Mitigating Cyber Attacks on Electric Vehicle Charging Networks in Public Infrastructure

Paritosh Biswas
https://orcid.org/0009-0000-4506-9827
Marwadi University, India

Sushil Kumar Singh
https://orcid.org/0000-0003-0030-5691
Marwadi University, India

Habib Khan
Gachon University, South Korea

ABSTRACT

The rapid adoption of Electric Vehicles (EVs) is transforming sustainable mobility and creating new demands for secure public charging infrastructure. The digital integration of EV charging networks creates vulnerabilities exposed to various cyber threats, including denial-of-service, malware, ransomware, and man-in-the-middle attacks are significant concerns. These vulnerabilities can lead to service disruption, financial loss, and reduced public trust. This chapter provides a comprehensive review of cybersecurity risks within the EV infrastructure, emphasizing the role

DOI: 10.4018/979-8-3373-3760-9.ch001

of AI-driven approaches in mitigating risks through the use of machine learning, anomaly detection, and adaptive defence strategies. Predictive analytics help identify and respond to emerging threats. The chapter also covers secure communication protocols and encryption mechanisms. Integration of predictive intelligence in the development of secure and resilient public EV infrastructure ensures operational continuity and trust in digital EV infrastructure.

INTRODUCTION

Smart cities are founded on the application of digital technologies and public infrastructural connectivity to develop the level of urban life, energy, and rational level of emissions. Electric Vehicles form one of those ecosystems, as they are pushing business to be profitable in the transport sector on the one hand and are in contact with the city public infrastructure literally all the time, such as charging points, traffic control system, and bus and tram network. This amount of connectivity renders EV communications systems vulnerable to cybersecurity threats and an attacker can disrupt the traffic pattern, control of energy, or privacy of personal data. This may also involve man-in-the-middle attack which may arise when EVs are attached to the public chargers via mobile apps or through a city Wi-Fi, which should be highly encrypted and authenticated. The unification of the artificial intelligence and Internet of Things (IoT) technologies to help in controlling the EV traffic and supply it with a source of power adds even more to the attack surface. The modern base of all EV systems is IoT and connects them to the automobiles, charge-up, grid, and personal mobile applications using the various sensors to monitor the battery level, navigation preserves, and service warnings. However, vulnerability of these IoT devices due to their interdependence nature poses a dangerous cybersecurity threat as the poorly secured IoT devices may be remotely accessed resulting to erroneous invoice or the unavailability of a service. Many of the Internet of Things architecture protocols suffer poor authentication and encryption which results in vulnerability to spoofing and denial of service attacks. In order to ensure the security of these networks we have to consider, the integrity of firmware and secure boot processes, software patches in time, anomaly detection using machine learning in real time. Smart EV networks are networks that are fully incorporated with EVs, charging infrastructure, energy providers and cloud platforms that interact using intelligent platforms and means of maximizing the charging, route planning, energy usage and predictive maintenance. These networks in spite of the benefits brought about have a high chance of being attacked by cyber-attacks that include data manipulation, denial-of-service, firmware hacking, and the man in the middle attack, all these expose them to the risk of losing their service interruption, monetary looting, and