Journal of Information Technology and Digital World (ISSN: 2582-418X)
www.irojournals.com/itdw/

Securing the Future of Mobility: Electric Vehicle Charging Infrastructure Protection

Rahul Kumar Jha[1], Sumina Neupane[2]

Department of Electrical Engineering, Western Regional Campus, Tribhuvan University, Pokhara, Nepal

E-mail: [1]rahul.752418@pasc.tu.edu.np, [2]pas075bel041@wrc.edu.np

Abstract

The rapid growth of electric vehicles (EVs) has spurred the need for a robust and secure charging infrastructure to ensure the future of mobility. This comprehensive study explores the critical topic of securing electric vehicle charging infrastructure, focusing on the protection of the vital component of the EV ecosystem. The study begins by providing an overview of the different types of EV charging infrastructure and the current state of deployment. It then examines the inherent challenges and vulnerabilities associated with EV charging infrastructure security, encompassing both physical threats, such as vandalism and theft, as well as cybersecurity threats, such as unauthorized access and data breaches. Existing security measures, including physical site design considerations and cybersecurity protocols, are reviewed, along with industry standards and regulations that provide guidance in this domain. The emerging technologies and strategies, such as blockchain, artificial intelligence, and secure communication protocols, that can enhance the protection of EV charging infrastructure are also explored in the study. Furthermore, it analyses relevant case studies illustrating real-world attacks on charging infrastructure, successful deployment stories, and the valuable lessons learned from these experiences. Finally, the paper outlines future directions and recommendations, including research needs, policy considerations, and stakeholder collaboration, aimed at establishing a secure and resilient EV charging ecosystem. By comprehensively addressing the security challenges surrounding EV charging infrastructure, the study aims to contribute to the advancement of effective measures and strategies to safeguard the future of mobility in an increasingly electrified world.

Keywords: Electric vehicles (EVs), Charging infrastructure, Security, Threats, Cybersecurity, Emerging technologies

DOI: https://doi.org/10.36548/jitdw.2023.3.005
Received: 06-07-2023. received in revised form: 07-08-2023, accepted: 23-08-2023, published: 06-09-2023

1. Introduction

A. Background on the Growth of Electric Vehicles (EVs)

The global automotive landscape has been undergoing a significant transformation with the increasing adoption and prominence of electric vehicles (EVs). Over the past decade, there has been a notable shift towards cleaner and more sustainable transportation options, driven by factors such as environmental concerns and advancements in battery technology. As governments, industries, and consumers recognize the urgency of reducing greenhouse gas emissions and combating climate change, electric vehicles have emerged as a crucial solution[1]. The growth of EVs can be attributed to several key factors. Firstly, heightened awareness of environmental issues, including air pollution and climate change, has prompted a shift away from traditional internal combustion engine (ICE) vehicles powered by fossil fuels. EVs offer a cleaner alternative with zero tailpipe emissions, contributing to improved air quality and reduced carbon emissions. Secondly, advancements in battery technology have greatly enhanced the performance and affordability of EVs. Innovations in lithium-ion batteries, coupled with economies of scale in production, have led to increased driving ranges, shorter charging times, and more competitive pricing. This has alleviated concerns about EVs' practicality and range limitations, making them a viable option for a wider range of consumers. Statistics and trends also reflect the rise in EV sales and market share[2].

B. Importance of Electric Vehicle Charging Infrastructure

While the growth of EVs is promising, the success of this transition relies heavily on the development of a robust electric vehicle charging infrastructure. Charging infrastructure plays a pivotal role in supporting widespread EV adoption by addressing key concerns that potential EV buyers might have[3]. The availability of reliable and accessible charging networks is essential for instilling confidence in consumers and eliminating "range anxiety," which refers to the fear of running out of battery power before reaching the charging station.

C. Need for Securing EV Charging Infrastructure

While the growth of EVs and charging infrastructure presents numerous benefits, it also introduces vulnerabilities that need to be addressed. Physical threats, such as vandalism, theft, and sabotage, can disrupt the functioning of charging stations and impact the overall user experience. Moreover, as charging infrastructure becomes increasingly interconnected and

reliant on digital systems, the risk of cybersecurity breaches rises[4]. Cybersecurity risks include unauthorized access to charging stations, data breaches that compromise user information, and potential attacks on the broader energy grid. Malicious actors could exploit vulnerabilities in charging infrastructure software and hardware to gain control, disrupt services, or compromise user data. Given the interconnected nature of the EV ecosystem, a breach in one part of the system that could have cascading effects.

2. Overview of Electric Vehicle Charging Infrastructure

A. Types of Charging Infrastructure

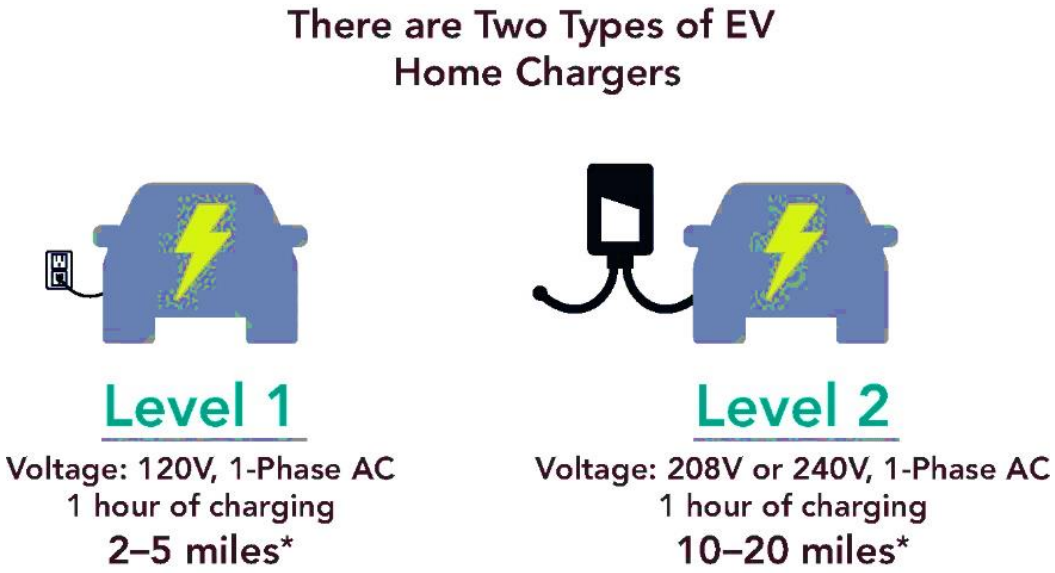

Figure 1. Types of EV home Chargers[5]

(i) Level 1 Charging

Level 1 charging as shown in Figure 1 above is the most basic form of EV charging and utilizes a standard household electrical outlet. This type of charging provides a low charging speed, typically delivering around 2 to 5 miles of range per hour of charging. While slow, it is suitable for scenarios where the vehicle is parked for an extended period, such as overnight

charging at home. Level 1 charging doesn't require any special equipment beyond a standard 120-volt outlet, making it widely accessible.

(ii) Level 2 Charging

Level 2 charging as shown in Figure 1 above requires dedicated charging equipment that operates on a 240-volt circuit. This type of charging offers a faster charging speed compared to Level 1, providing approximately 10 to 30 miles of range per hour of charging. Level 2 charging stations are commonly found in residential settings, workplaces, commercial areas, and public spaces. Due to their higher charging power, Level 2 stations can significantly reduce charging times while still being relatively affordable to install.

(iii) DC Fast Charging

DC fast charging, also known as Level 3 charging, is designed for rapid charging on the go. This type of charging employs direct current (DC) to quickly replenish an EV's battery. [6].

B. Current State of EV Charging Infrastructure Deployment

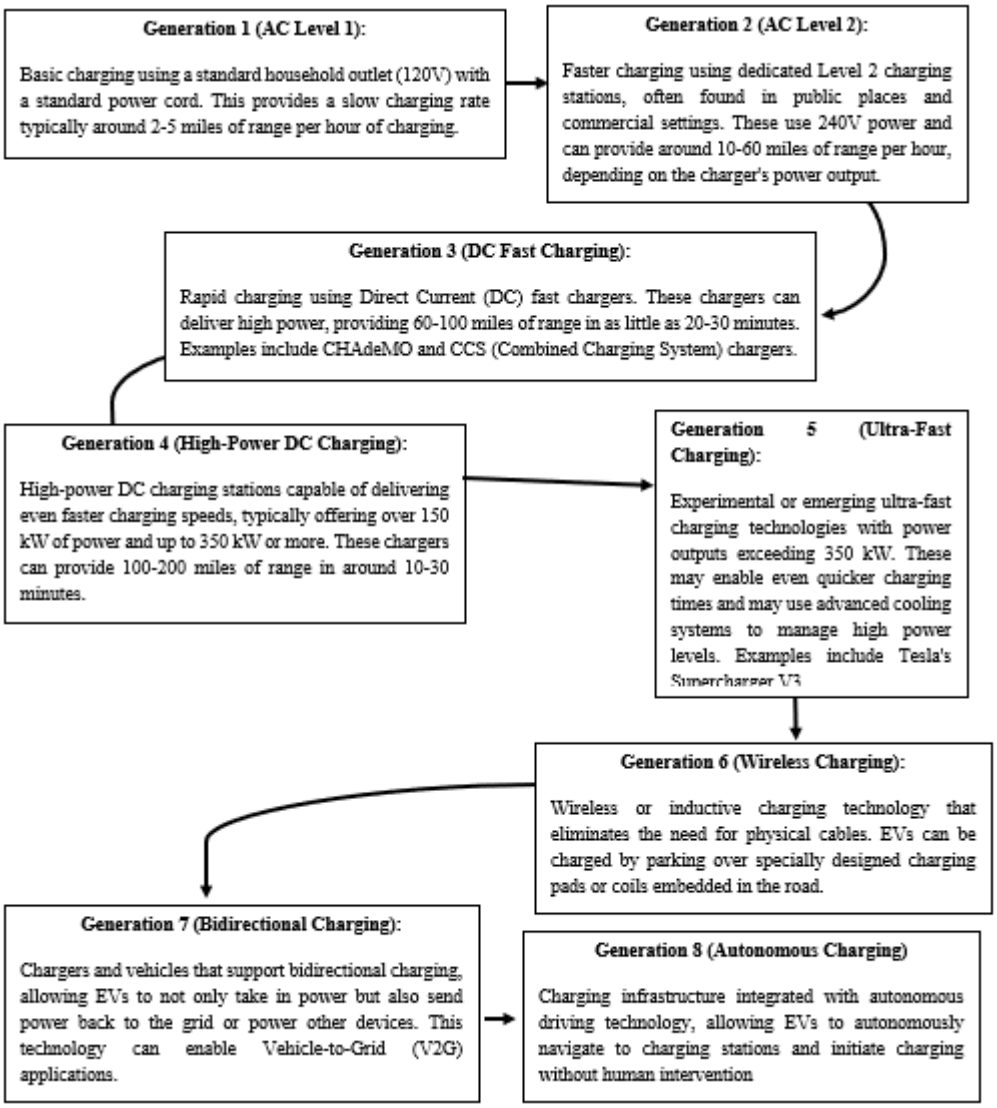

Figure 2. Current State of EV Charging Infrastructure Deployment

C. Challenges and Vulnerabilities in EV Charging Infrastructure Security

(i) Physical Security Challenges

EV charging stations are vulnerable to physical threats such as vandalism, theft, and tampering. Charging cables, connectors, and other equipment can be damaged or stolen, disrupting the charging process and inconveniencing users. To address these challenges, secure

physical designs, durable materials, and monitoring systems are necessary to deter and detect malicious activities[7].

(ii) Cybersecurity Challenges

As charging infrastructure becomes more connected and relies on digital systems for payment processing, monitoring, and remote management, the cybersecurity risks increase[8]. Unauthorized access to charging stations can result in service disruption or the manipulation of charging processes. Data breaches could compromise user information, including payment details and personal data. To mitigate these challenges, robust cybersecurity measures are essential. This includes implementing encryption, secure authentication mechanisms, regular software updates, and continuous monitoring of network traffic to detect and prevent unauthorized access and potential cyber threats[9].

Addressing these challenges and vulnerabilities is crucial to ensure the reliability and trustworthiness of EV charging infrastructure. By adopting comprehensive security measures that encompass both physical and cybersecurity aspects, stakeholders can create a safe and secure environment for users and contribute to the continued growth and success of electric vehicle adoption.

3. Threats to Electric Vehicle Charging Infrastructure[9]

Category	Threats and Challenges	Potential Impact
A. Physical security threats	• Vandalism and theft	• Loss of public confidence in EV infrastructure • Decreased utilization of charging stations
	• Sabotage and tampering	• Safety risks for users and vehicles. • Disruption of charging networks.

B. Cybersecurity threats	• Unauthorized access and control	• Malicious control over charging infrastructure. • Compromised energy grid stability.
	• Data breaches and privacy concerns	• Identity theft and financial losses. • Legal and reputational consequences.
C. Potential impact on EV adoption and usage	• Limited charging options for users	• Discouragement of potential EV buyers. • Reluctance to travel long distances.
	• Negative portrayal in the media • Investment uncertainty for stakeholders	• Stifled growth of the EV market. • Slower development of charging infrastructure.

Table 1. Threats to EV Charging Infrastructure

The Table.1 list the different types of threats that affect the electric vehicle infrastructure

4. Existing Security Measures for EV Charging Infrastructure

A. Physical Security Measures

(i) Site Selection and Design Considerations

Secure locations play a crucial role in deterring physical threats. High-visibility areas, well-lit environments, and locations near high-traffic areas reduce the likelihood of vandalism and theft. Proximity to security personnel, surveillance cameras, and other public spaces enhances the safety of charging stations[10].

(ii) Surveillance Systems and Access Control

1. Surveillance cameras monitor charging stations and their surroundings, providing real-time visual data that can aid in identifying potential threats.
2. Alarms and physical barriers prevent unauthorized access and raise alerts in case of suspicious activities.
3. Automated access control systems limit usage to authorized users and enhance security during off-hours.

(iii) Vehicle Identification and Authentication Mechanisms

1. RFID tags or unique identifiers on vehicles ensure that only authorized users can access charging services.
2. Authentication processes establish the identity of the vehicle and its owner before allowing charging sessions to commence, preventing unauthorized usage.

B. Cybersecurity Measures

(i) Secure Communication Protocols:

1. Encrypted connections and protocols like TLS protect data transferred between EVs, charging stations, and backend systems from interception and tampering.
2. Encryption ensures that sensitive data remains confidential during transmission.

(ii) Encryption and Authentication Mechanisms

1. Encryption algorithms protect sensitive information stored on charging infrastructure systems, preventing unauthorized access.
2. Strong authentication methods like digital certificates or biometric verification ensure that only authorized parties can interact with the charging infrastructure.

(iii) Intrusion Detection and Prevention Systems[11]

1. Intrusion detection systems monitor network traffic for anomalies and signs of cyberattacks, raising alarms or taking preventive actions when suspicious behavior is detected.

2. Firewalls and network segmentation isolate critical components of the charging infrastructure, reducing the attack surface and preventing lateral movement of threats.

C. Industry Standards and Regulations for EV Charging Infrastructure Security[12]

1. ISO 15118: This international standard defines a communication protocol between EVs and charging infrastructure, including security measures to protect data exchange during charging.
2. IEC 61851: This standard provides requirements for the safety and performance of EV charging equipment, including considerations for electrical safety and communication security.
3. Regional Regulations: Various countries and regions have established regulations that mandate cybersecurity requirements, data privacy protection, and interoperability standards for EV charging infrastructure.

5. Emerging Technologies and Strategies for EV Charging Infrastructure[13]–[16]

A. Blockchain Technology for Secure Transactions and Data Management

Description: Blockchain technology offers a decentralized and tamper-resistant ledger for recording transactions. It utilizes smart contracts to automate processes, ensuring secure charging session initiation, payment verification, and data management.

Benefits: Secure Transactions and Payment Processing: Blockchain enhances security by providing a transparent and immutable record of transactions, reducing the risk of fraudulent activities.

Tamper-resistant data management: Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity of charging session records and user information.

Transparent and fraud-resistant system: Transparency in blockchain transactions makes it easier to detect any unauthorized access or anomalies, preventing fraudulent behavior.

B. Artificial Intelligence and Machine Learning For Threat Detection And Response

Description: AI and ML algorithms analyze large datasets generated by EV charging stations to identify anomalies in charging behavior. The algorithms enable a real-time threat detection and predictive maintenance.

Benefits: Real-time Threat Detection and Response: AI and ML systems continuously monitor charging data and can quickly identify unusual patterns or security breaches, allowing for immediate action.

Anomaly Detection and Predictive Maintenance: These technologies help prevent potential issues by identifying and addressing them before escalating , and ensuring the reliability of the charging infrastructure.

Adaptability to New and Evolving Threats: AI and ML models can adapt and learn from new threat patterns, making them effective against evolving security challenges.

C. Secure Communication Protocols and Network Architectures

Description: Utilizing secure communication protocols such as Transport Layer Security (TLS) encrypts data transmission between charging stations and backend systems. Virtual Private Networks (VPNs) establish private communication channels to protect user data.

Benefits: Encrypted and Secure Data Transmission: TLS encryption prevents unauthorized parties from intercepting and accessing sensitive data during transmission, ensuring data privacy.

Prevention of Unauthorized Access and Data Breaches: Secure protocols and VPNs safeguard against unauthorized access, reducing the risk of data breaches and cyberattacks.

Establishment of Private and Secure Communication Channels: VPNs create a secure tunnel for data transfer, protecting user information from potential threats on public networks.

D. Integration with Smart Grid Infrastructure for Enhanced Security

Description: Integrating EV charging with smart grids enables dynamic load management and energy optimization. Secure authentication mechanisms ensure that only authorized users have access to the charging infrastructure

Benefits: Dynamic Load Management and Energy Optimization: Smart grids can balance the load on the electrical grid, preventing overloads and optimizing energy distribution. This enhances the overall stability and efficiency of the grid.

Secure Authentication for Authorized Access: Only authorized users can access and use the charging infrastructure, reducing the risk of misuse or unauthorized access.

Real-time Monitoring and Response to Anomalies: Smart grid integration allows for real-time monitoring of charging stations and immediate response to any anomalies or issues, improving the security and reliability of the charging ecosystem.

6. Design of Protection System in EV Charging Infrastructure

The figure 3 is the step-by-step approach for designing a protection system in the EV charging infrastructure:

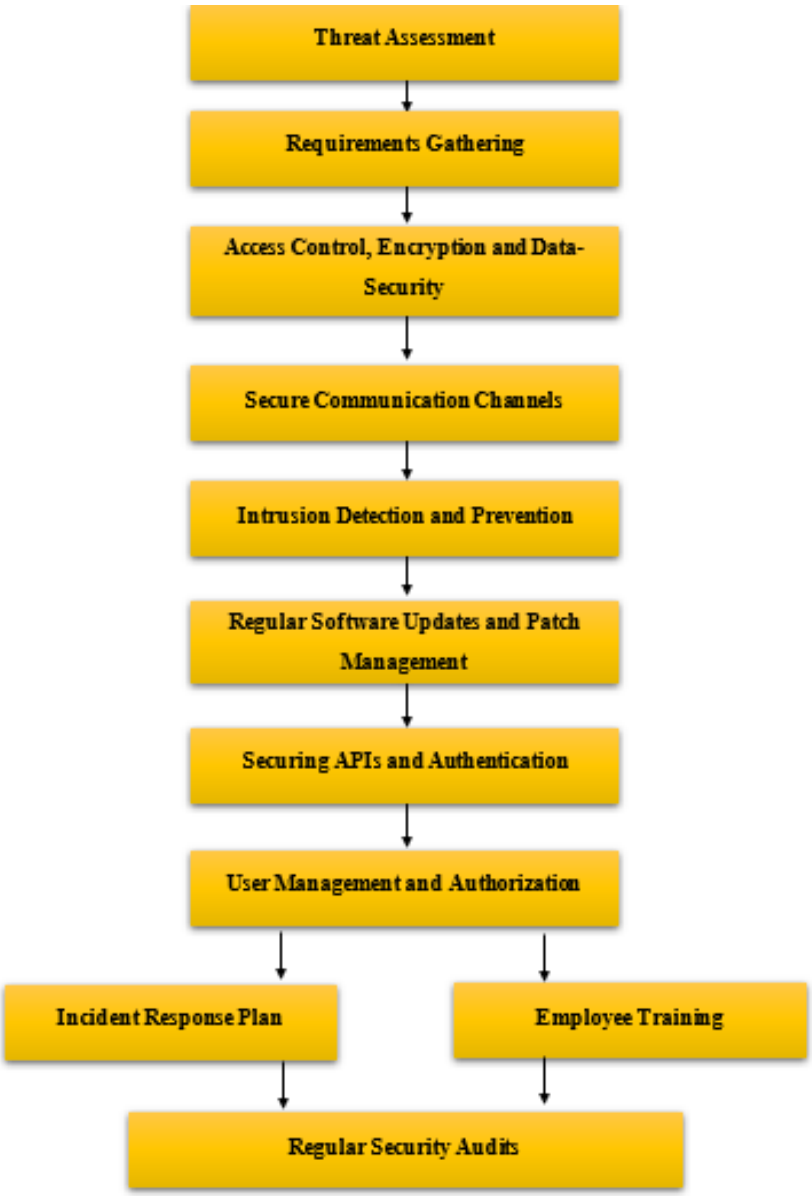

Figure 3. Protection System for EV Charging Infrastructure: Step by Step Approach

7. Application of Machine Learning, Secure Communication Protocols and Integration with the Smart Grid for Enhancing Security and Privacy in EV Charging Station[17], [18]

A. Machine Learning (ML)

Real-time Threat Detection: ML algorithms analyse large datasets generated by charging stations to identify anomalies in charging behaviour. This enables real-time detection of potential security breaches.

Predictive Maintenance: ML can predict and address issues before escalating, and ensuring the reliability of charging infrastructure as well as preventing vulnerabilities from being exploited.

Application	Description and Benefits	Machine Learning Algorithms
Predictive Maintenance	Predicting equipment failures and maintenance needs based on data from charging stations, reducing downtime and improving reliability.	Regression, Decision Trees, Random Forest, Neural Networks, LSTM
Anomaly Detection	Detecting unusual or suspicious behavior in charging stations, such as unauthorized access or cyberattacks, for early intervention.	Isolation Forest, One-Class SVM, Autoencoders, LSTM
User Authentication	Enhancing user security through multi-factor authentication, biometrics, and behavioral analysis for access control.	Machine Learning for Biometrics (e.g., face recognition), Behavioral Analytics
Privacy Protection	Protecting user data and identity through encryption and anonymization techniques to prevent data breaches and privacy violations.	Differential Privacy, Homomorphic Encryption, Data Masking
Intrusion Detection	Identifying and responding to cyber threats and network intrusions in real-time to safeguard the charging infrastructure.	Deep Learning for Network Intrusion Detection, XGBoost, SVM
Dynamic Load Management	Optimizing charging station usage and energy distribution in response to real-time demand, reducing grid stress and costs.	Reinforcement Learning, Q-learning, Proximal Policy Optimization
Fraud Detection	Detecting fraudulent activities related to payments, user accounts, and charging sessions, improving financial security.	Machine Learning for Fraud Detection, Pattern Recognition
Grid Integration Security	Ensuring the secure integration of charging stations with the smart grid to prevent grid vulnerabilities and cyberattacks.	Security Policy Enforcement, Intrusion Detection, Bayesian Networks

B. Blockchain Technology

Secure Transactions: Blockchain ensures secure and tamper-resistant transactions for EV charging payments. Smart contracts can automate payment verification, reducing the risk of fraudulent activities.

Tamper-Resistant Data: Charging session data recorded on the blockchain is immutable and transparent. This prevents unauthorized access and tampering of charging records, enhancing the integrity of the system.

Transparency and Fraud Prevention: The transparency of blockchain transactions makes it easier to detect any unauthorized or suspicious activity, reducing the chances of fraud.

C. Secure Communication Protocols

Advanced protocols used for securing EV charging stations include OCPP, OCPI, ISO 15118, PKI, OAuth 2.0, SCAP, SOAP/REST with security extensions, WebSocket with WSS, and blockchain-based protocols. These protocols provide secure communication, authentication, authorization, and protection against cyber threats, enhancing the overall security of EV charging infrastructure.

D. Integration with Smart Grid

Dynamic Load Management: Integration with the smart grid allows for dynamic load management, preventing overloads and optimizing energy distribution. This enhances the overall stability of the grid and reduces the risk of disruptions.

Secure Authentication: Only authorized users can access and use the charging infrastructure, reducing the risk of misuse or unauthorized access.

E. Comparison of Existing and Emerging Technology

The graphical representation in figure 4 and the data table in table 2 below compare and contrast the conventional methods of EV charging as well as the emerging technologies that integrate block chain, machine learning, advanced protocols, and the smart grid for enhancing security and preventing vulnerabilities in the charging station on the basis of the security, accuracy, and time consumed.

Table 2. Comparison of Emerging and Existing Technology

Term	Emerging Technology	Existing Technology
Security	92%	78%
Accuracy	96%	85%
Time Consumed	60 minutes	120 minutes

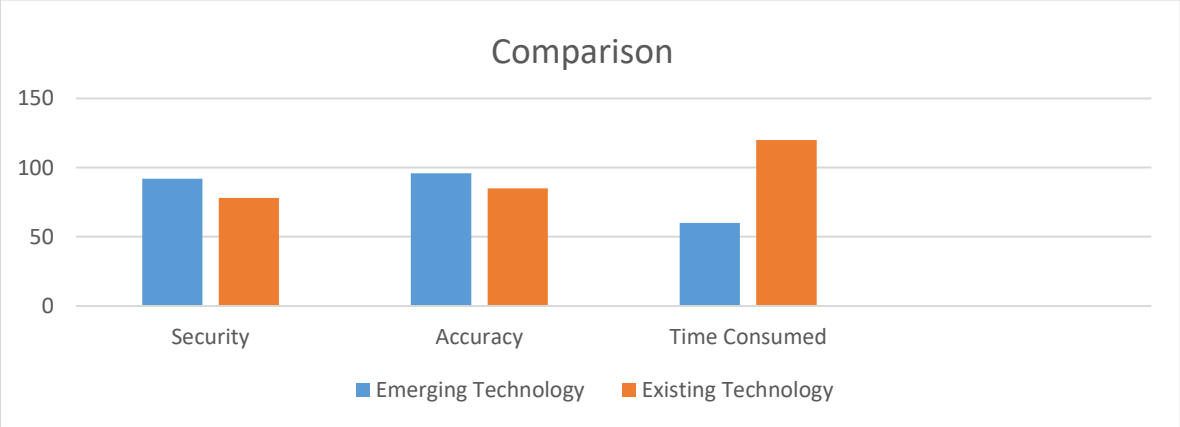

Figure 4. Graphical Representation on basis of Security, Accuracy, Time Consumed

8. Key Insights

1. Security is Crucial for EV Charging Infrastructure: The growth of electric vehicles depends on secure charging infrastructure. Addressing security concerns is essential to build trust among users and promote widespread EV adoption.

2. Diverse Threat Landscape: EV charging infrastructure faces a range of threats, including physical risks like vandalism and theft, as well as cybersecurity risks such as unauthorized access and data breaches. Comprehensive security measures are needed to protect against these threats.

3. Charging Infrastructure Types: Understanding the different levels of charging infrastructure (Level 1, Level 2, DC fast charging) is essential for implementing appropriate security measures, as each has unique requirements and vulnerabilities.

4. Data Privacy is Paramount: Protecting user data and privacy is a critical aspect of EV charging security. Anonymization techniques and secure data handling are vital to maintain user trust.

5. Emerging Technologies Hold Promise: Blockchain, AI, and machine learning offer innovative solutions for enhancing security and privacy in EV charging. These technologies can help detect anomalies, secure communications, and improve authentication.

6. Collaboration is Key: Collaboration between stakeholders, including industry players, regulators, and security experts, is crucial for developing comprehensive security guidelines, sharing threat intelligence, and establishing best practices.

7. Policy and Regulation Play a Vital Role: Robust cybersecurity and privacy regulations, along with industry standards, provide a framework for secure EV charging infrastructure. Enforcing these regulations is essential to ensure compliance across the ecosystem.

8. Research and Development are Ongoing: Continuous research and development efforts are needed to address emerging security challenges, improve authentication mechanisms, and stay ahead of evolving threats.

9. Conclusion

The transition to electric vehicles (EVs) is a significant shift towards cleaner and more sustainable transportation, making the security and reliability of EV charging infrastructure crucial. The diverse threat landscape, including physical risks like vandalism and theft, necessitates a multifaceted security approach, including secure charging locations, robust surveillance systems, advanced authentication methods, encryption, intrusion detection systems, and regular security audits. Technological innovations like blockchain, AI, and machine learning offer opportunities to detect anomalies, secure communications, and enhance authentication methods, bolstering the resilience of charging networks. Collaboration among stakeholders, including infrastructure operators, vehicle manufacturers, regulators, and

cybersecurity experts, is essential for ensuring the security of EV charging infrastructure. Policy and regulatory frameworks play a crucial role in shaping the security landscape, enacting and enforcing cybersecurity and privacy regulations, and introducing industry standards and certification programs.

References

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[2] J. Cao, X. Chen, R. Qiu, and S. Hou, "Electric vehicle industry sustainable development with a stakeholder engagement system," Technol Soc, vol. 67, Nov. 2021, doi: 10.1016/j.techsoc.2021.101771.

[3] "Security architecture for electric vehicle charging infrastructure," 2019. [Online]. Available: https://encs.eu/documents

[4] S. Mishra et al., "A comprehensive review on developments in electric vehicle charging station infrastructure and present scenario of India," Sustainability (Switzerland), vol. 13, no. 4, pp. 1–20, Feb. 2021, doi: 10.3390/su13042396.

[5] "MCE Community Choice Energy ."

[6] M. Brenna, F. Foiadelli, C. Leone, and M. Longo, "Electric Vehicles Charging Technology Review and Optimal Size Estimation," Journal of Electrical Engineering and Technology, vol. 15, no. 6, pp. 2539–2552, Nov. 2020, doi: 10.1007/s42835-020-00547-x.

[7] M. S. Mastoi et al., "An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends," Energy Reports, vol. 8. Elsevier Ltd, pp. 11504–11529, Nov. 01, 2022. doi: 10.1016/j.egyr.2022.09.011.

[8] J. Leijon and C. Boström, "Charging Electric Vehicles Today and in the Future," World Electric Vehicle Journal, vol. 13, no. 8. MDPI, Aug. 01, 2022. doi: 10.3390/wevj13080139.

[9] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, “Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective,” IEEE Access, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 214434–214453, 2020. doi: 10.1109/ACCESS.2020.3041074.

[10] Z. Pourmirza and S. Walker, “Electric Vehicle Charging Station: Cyber Security Challenges and Perspective,” in 2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE), 2021, pp. 111–116. doi: 10.1109/SEGE52446.2021.9535052.

[11] J. Andrews, T. L. Polmateer, J. P. Wheeler, D. L. Slutzky, and J. H. Lambert, “Enterprise Risk and Resilience of Electric-Vehicle Charging Infrastructure and the Future Mobile Power Grid,” Current Sustainable/Renewable Energy Reports, vol. 7, no. 1, pp. 9–15, 2020, doi: 10.1007/s40518-020-00144-6.

[12] H. S. Das, M. M. Rahman, S. Li, and C. W. Tan, “Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review,” Renewable and Sustainable Energy Reviews, vol. 120, p. 109618, 2020, doi: https://doi.org/10.1016/j.rser.2019.109618.

[13] H. Lee, H. K. School, and A. Clark, “Charging the Future: Challenges and Opportunities for Electric Vehicle Adoption Faculty Research Working Paper Series,” 2018. [Online]. Available: https://www.hks.harvard.edu/research-insights/publications?f%5B0%5D=publication_types%3A121

[14] T. Vairo, M. Pettinato, A. P. Reverberi, M. F. Milazzo, and B. Fabiano, “An approach towards the implementation of a reliable resilience model based on machine learning,” Process Safety and Environmental Protection, vol. 172, pp. 632–641, 2023, doi: https://doi.org/10.1016/j.psep.2023.02.058.

[15] M. S. Choi, “MACHINE LEARNING FOR RESILIENT AND SUSTAINABLE ENERGY SYSTEMS UNDER CLIMATE CHANGE,” Aug. 2023, doi: 10.25394/PGS.23898003.v1.

[16] M. Shahzad, A. Qadir, N. Ullah, Z. Mahmood, N. M. Saad, and S. S. A. Ali, “Optimization of On-Grid Hybrid Renewable Energy System: A Case Study on Azad

Jammu and Kashmir," Sustainability (Switzerland), vol. 14, no. 10, May 2022, doi: 10.3390/su14105757.

[17] Rahul Kumar Jha, "Cybersecurity and Confidentiality in Smart Grid for Enhancing Sustainability and Reliability," Recent Research Reviews Journal, vol. 2, no. 2, pp. 215–241, Dec. 2023, doi: 10.36548/rrrj.2023.2.001.

[18] Rahul Kumar Jha, "Strengthening Smart Grid Cybersecurity: An In-Depth Investigation into the Fusion of Machine Learning and Natural Language Processing," Journal of Trends in Computer Science and Smart Technology, vol. 5, no. 3, pp. 284–301, Sep. 2023, doi: 10.36548/jtcsst.2023.3.005.

Author's biography

Rahul Kumar Jha

Rahul Kumar Jha, with a Bachelor's degree in Electrical Engineering from Tribhuvan University, has practical experience in data visualization, supply chain management, and technical expertise. He seeks opportunities to expand knowledge through online platforms and participates in specialized courses. With a strong educational foundation and dedication to excellence, he inspires and mentors' individuals in STEM fields.

Sumina Neupane

Sumina Neupane is a passionate electrical engineering graduate from Kathmandu, Nepal, with a strong interest in power electronics, renewable energy, and research. After graduating with honors, Sumina embarked on a promising career in electrical engineering. Her innovative approach and problem-solving abilities made her a valuable asset in designing and implementing various electrical projects. She excelled academically at Paschimanchal Campus in Pokhara, completing her Bachelor's degree in Electrical Engineering in 2023.