COMSM0120_2024_TB2

Security of Industrial Control System

Individual Assignment

Topic:
Analysis of EV Charging on the Smart Grid

Student No: 2451975

Word Count: 2936

Faculty of Engineering
School of Computer Science
University of Bristol



Contents

1 Introduction **3**

2 EV Charging and Smart Grid Infrastructure **3**
- 2.1 Home Charging . . . 4
- 2.2 Commercial Car Parks . . . 4
- 2.3 Communication Networks . . . 5

3 Security Vulnerabilities **6**
- 3.1 Key Vulnerabilities in Protocols . . . 6
  - 3.1.1 CAN Protocol . . . 6
  - 3.1.2 3G/4G Networks . . . 6
  - 3.1.3 LAN (Local Area Network) . . . 7
- 3.2 Key Vulnerabilities in Components . . . 8
  - 3.2.1 Charging Management System (CMS) . . . 8
  - 3.2.2 Local Power Distribution Unit (Including SCADA) . . . 9
  - 3.2.3 Smart Meters . . . 9

4 Attack Methods **10**
- 4.1 CAN Protocol . . . 10
- 4.2 3G/4G Networks . . . 11
- 4.3 LAN(Local Area Network) . . . 11
- 4.4 Charging Management System (CMS) . . . 12
- 4.5 Local Power Distribution Unit (Including SCADA) . . . 12
- 4.6 Smart Meters . . . 13

5 Mitigation Strategies **14**
- 5.1 Can Protocol . . . 14
- 5.2 3G/4G . . . 15
- 5.3 LAN(Local Area Network) . . . 16
- 5.4 Charging Management System (CMS) . . . 17
- 5.5 Local Power Distribution Unit (Including SCADA) . . . 18
- 5.6 Smart Meter Security . . . 19

6 Conclusion **20**

7 Future Works **20**

1 Introduction

The growing popularity of electric vehicles is driving a rapid increase in charging stations. These networks use modern communication systems and smart grid connections to improve efficiency and promote sustainability. However, this development also poses security risks. Because these systems rely on network communication, cloud management, and two-way power flow, they can be vulnerable to cyber attacks that could disrupt the power grid, compromise user data, or damage system integrity.

This report looks at the weak points in EV charging networks. It highlights potential risks in how these systems communicate, verify users, and manage energy. Various types of attack, including unauthorized access, denial-of-service attacks, and firmware manipulation, can seriously undermine the security and reliability of these networks. To protect the EV charging infrastructure from these evolving cyber threats, it is crucial to implement strong security measures.

2 EV Charging and Smart Grid Infrastructure

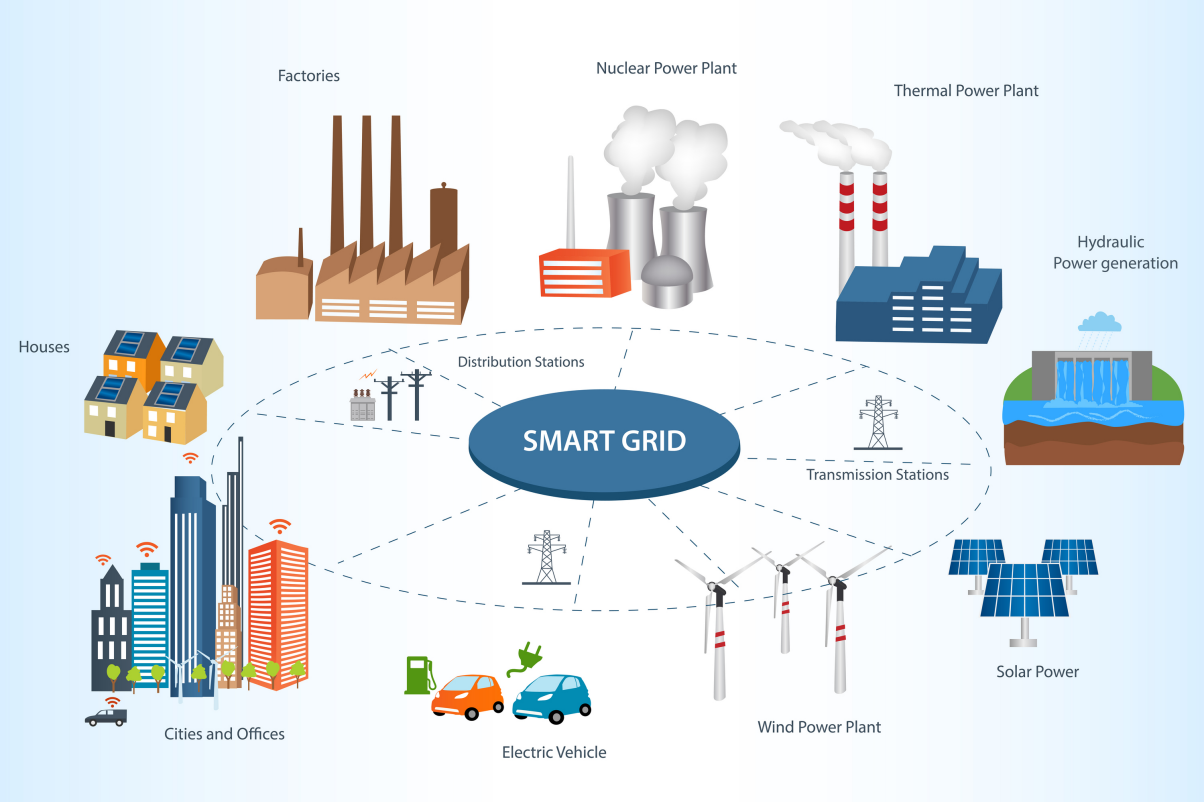


Figure 1: Smart Grid Ecosystem

2.1 Home Charging

Home charging is currently the most common means of charging electric cars. EV owners with access to a private parking space that can be equipped for charging can charge overnight, which is not only convenient but also typically takes advantage of lower electricity prices while demand is relatively low[1]. Home-based EV charging uses smart meters and Wi-Fi/4G communication with energy providers. These systems require authentication protocols to prevent unauthorized access. However, their connectivity to the smart grid, cloud-based platforms, and wireless networks exposes them to cybersecurity threats, including unauthorized access, data interception, and remote manipulation.

Component	Function
EV Charging Station (EVCS)	Connects to vehicles via CAN protocol.
Smart Meter	Tracks grid consumption and V2G returns via 3G/4G.
Distribution Panel	Manages power flow between grid, solar, and EV.
Solar Panels	Generate renewable energy for home/EV use.

Table 1: Components of Home EV Charging Systems

2.2 Commercial Car Parks

In commercial car parks, a centralized Charging Management System (CMS) manages hundreds of EVCS units via a local LAN, ensuring efficient scheduling and remote control. The Local Power Distribution Unit, integrated with SCADA systems, regulates and monitors power flow between the grid and chargers, while smart meters track energy usage for accurate billing and grid stability. This integrated infrastructure optimizes energy distribution and reliability across the charging network[2].

Component	Function
Charging Management System (CMS)	Centralized server managing hundreds of EVCS via LAN.
Local Power Distribution Unit	Includes SCADA systems for grid interaction.
Smart Meters	Track energy usage for billing and grid stability.

Table 2: Components of Commercial Car Parks

2.3 Communication Networks

In electric vehicles, the CAN protocol enables real-time communication between the EV and its charging station, exchanging critical data like battery status and charging commands. However, since CAN was designed primarily for speed and reliability, it lacks built-in security features, leaving it vulnerable to potential cyber-attacks if accessed improperly[3]. 3G/4G networks revolutionize mobile communication with high-speed, all-IP connectivity across technologies like LTE and WiMAX. While their open architecture supports seamless services like smart meter data in EV applications, it also brings security risks due to greater exposure and complex links[4]. LANs connect the Charging Management System (CMS) to EV Charging Stations, enabling quick, reliable data transfer for efficient energy management. Robust security and frequent vulnerability checks are essential to prevent breaches[5].

Protocols	Function
CAN	The CAN protocol enables real-time data exchange between the EV and its charging station.
3G/4G	3G/4G networks mark a significant leap in mobile communication by providing high-speed, all-IP connectivity.
LAN	Local area networks (LANs) provide the critical backbone connecting the Charging Management System (CMS).

Table 3: Components of Commercial Car Parks

3 Security Vulnerabilities

3.1 Key Vulnerabilities in Protocols

3.1.1 CAN Protocol

- CAN networks typically lack proper segmentation, meaning all ECUs are connected to the same bus. Without segmentation, attacks can propagate throughout vehicle network.
- CAN protocol does not implement device authentication mechanisms. Any device connected to the CAN bus is trusted by default.
- Attackers can send unauthorized control commands to modify charging behavior.
- CAN messages follow predictable patterns and structures. Attackers can analyze these patterns to develop targeted attacks that blend in with normal traffic[6].

3.1.2 3G/4G Networks

- Many EV charging stations use 3G/4G networks without end-to-end encryption, allowing attackers to intercept sensitive information.
- The use of outdated protocols in 3G/4G communications can expose EV charging infrastructure to interception attacks.
- Vulnerabilities in 3G/4G protocols can be exploited to perform MITM attacks. These attacks can compromise the integrity of communications between EVs, charging stations, and backend systems.
- EV users can be targeted with phishing SMS aka Smishing messages designed to steal credentials or install malware on their devices[7].

3.1.3 LAN (Local Area Network)

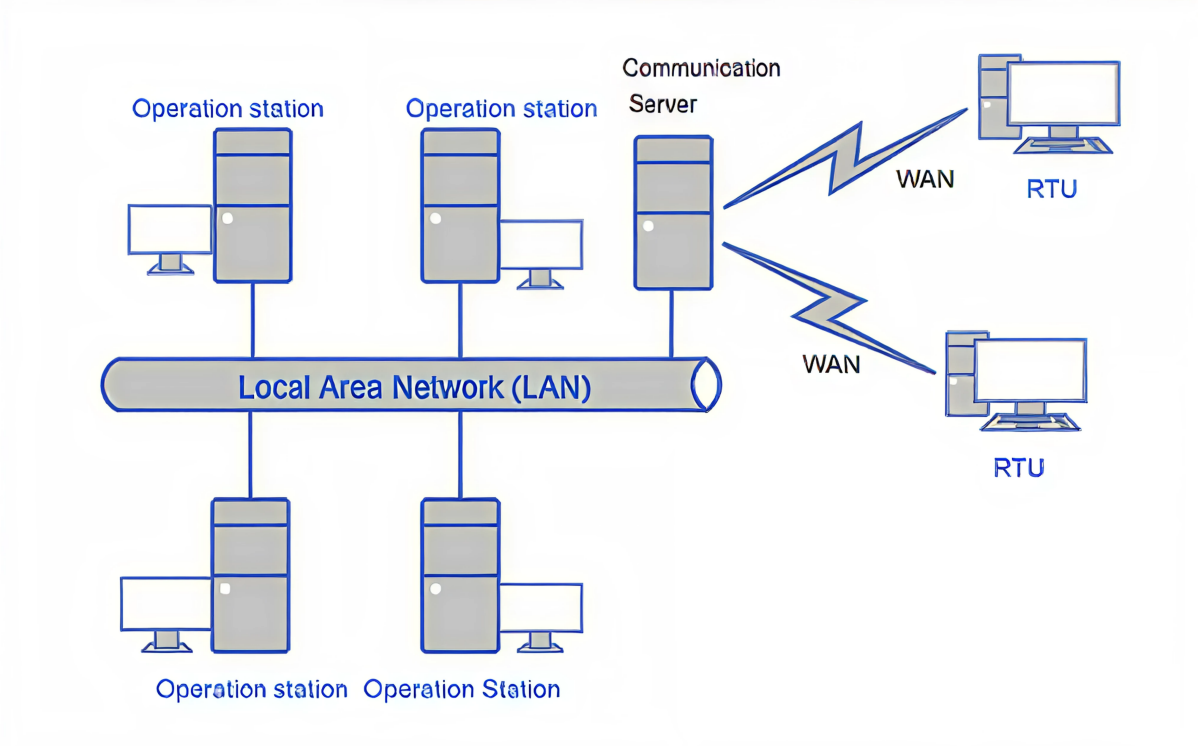


Figure 2: Distributed SCADA system

- In unsegmented LANs, a single breach can let attackers move laterally, risking the compromise of the entire network. Attackers can manipulate control systems to disrupt power distribution, inject false data, or halt industrial processes.
- Open ports or insecure services (e.g., Telnet, FTP) with weak authentication mechanisms can be exploited by attackers. These services can provide attackers with entry points to modify configurations, exfiltrate data, or disrupt operations.
- Many industrial systems provide remote access for maintenance and monitoring using insecure methods. Attackers can exploit these remote access points to gain entry to the control network.
- Common SCADA protocols like Modbus, Profibus, and DNP3 lack essential security features such as encryption, authentication, and integrity checks when implemented over LANs[8].

3.2 Key Vulnerabilities in Components

3.2.1 Charging Management System (CMS)

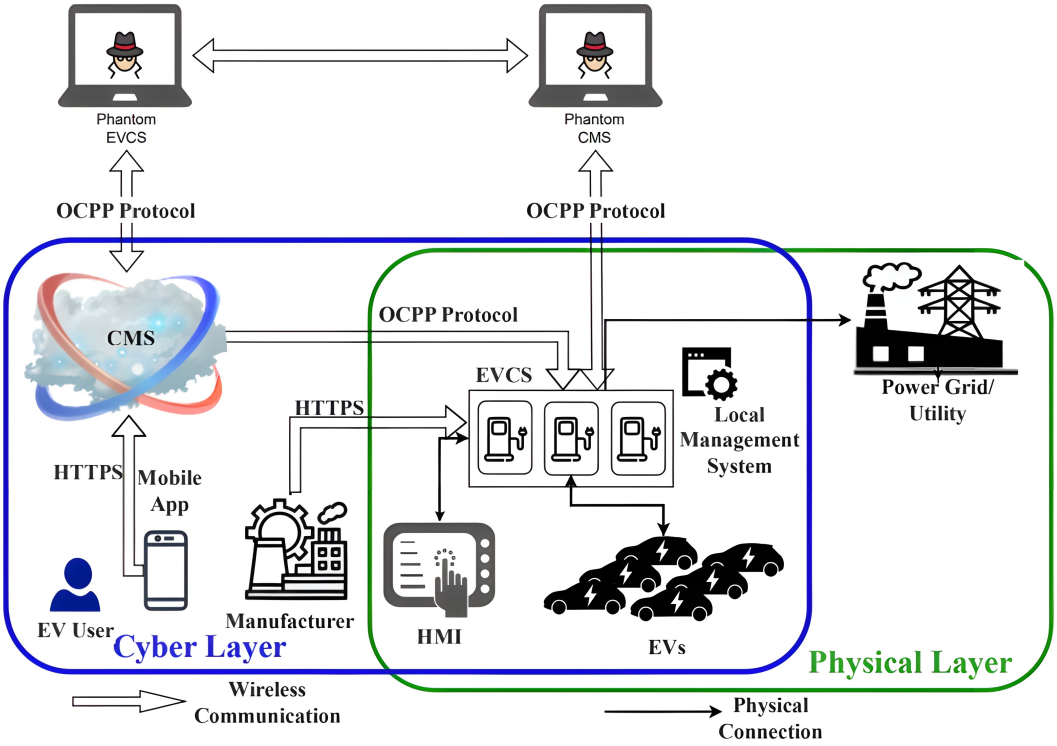


Figure 3: EV charging ecosystem's cyber/-physical layers

- The OCPP backend uses only the EVCS ID for authentication, which can be easily obtained by attackers. CWE-284 (Improper Access Control), CWE-287 (Improper Authentication)
- Attackers can spoof legitimate EVCS using phantom EVCS, gaining the same level of access as real EVCS. This allows attackers to hijack communications and impersonate legitimate charging stations. CWE-923 (Improper Restriction of Communication Channel to Intended Endpoints)
- No limits on the number of parallel connections from phantom EVCS using the same legitimate EVCS ID. Could cause DoS by overloading backend resources.
- Authentication relies solely on the EVCS ID, which is easily obtainable. This single-factor authentication makes it easier for attackers to compromise systems.CWE-654 (Reliance on Single Factor in a Security Decision)[9].

3.2.2 Local Power Distribution Unit (Including SCADA)

- Older SCADA protocols like DNP3 and Modbus typically do not employ encryption for data transmission. These protocols often rely on simple authentication methods that can be easily bypassed.
- Many power distribution systems have evolved organically, resulting in complex network architectures where SCADA systems may not be properly isolated from corporate networks or the internet. Attackers who gain access to less secure parts of the network can pivot to target SCADA components.
- SCADA systems in power distribution often run on specialized hardware and software that may not receive timely updates. This can leave known vulnerabilities unaddressed. Attackers exploiting these vulnerabilities could potentially disrupt power flow or cause equipment damage.
- Many power distribution SCADA components are located in remote substations. These locations may lack adequate physical security measures such as locks, surveillance cameras, or intrusion detection systems[10].

3.2.3 Smart Meters

- Smart meters communicating over wireless networks (like 3G/4G) may be vulnerable to eavesdropping if encryption is weak or absent. Attackers can monitor transmission patterns to infer information about power consumption and user presence.
- The Change and Transmit (CAT) policy, where smart meters transmit only when there's a significant power consumption change, creates predictable communication patterns that can be exploited.
- Attackers with access to the firmware update mechanism could upload customized firmware containing malware. This could give them control over the smart meter's operations[11].
- Attackers identify weak smart meters by analyzing network structures and intercepting unencrypted wireless communications. Using tools like wireless sniffers or physical access, they gather data, study its structure and security, and create fake packets to manipulate meter readings or measurements[12].

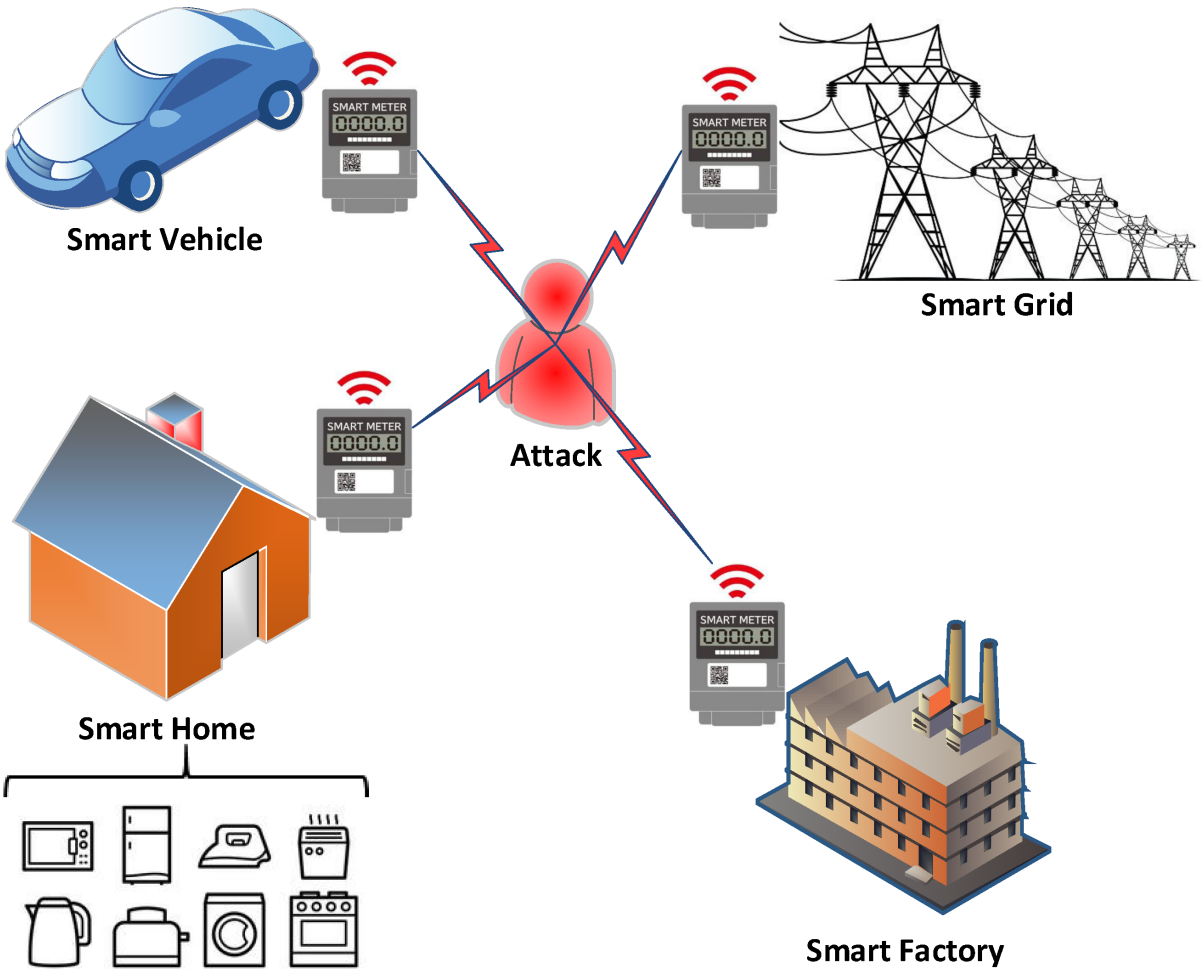


Figure 4: Smart meter with attack existence

4 Attack Methods

4.1 CAN Protocol

- Sniffing Attacks: Attackers monitor CAN bus traffic to collect sensitive information about vehicle operations, control systems, and potentially personal data. Can lead to privacy breaches and enable subsequent targeted attacks.
- Frame Falsifying Attacks: Attackers create and send counterfeit CAN frames to manipulate vehicle behaviour or trigger specific actions. Can cause unauthorized control of vehicle functions.
- Denial-of-Service (DoS) Attacks: Attackers overwhelm the CAN bus with high-priority messages, preventing legitimate communications. Can disrupt vehicle operations and safety-critical systems by blocking normal message transmission.

- Bus-Off Attacks: Attackers force an ECU into bus-off state by causing excessive errors, potentially to isolate it from the network. Can disable safety-critical systems or create opportunities for other attack vectors[13].

4.2 3G/4G Networks

- Attackers can position themselves between SCADA devices and the control center, using rogue access points or compromised networks to intercept and relay communications. i.e MiTM.
- Attackers exploit weak authentication mechanisms in EVCS that use 3G/4G for backhaul communications. They may brute-force credentials or exploit default configurations.
- Attackers intercept or modify pricing information transmitted over 3G/4G networks between charging stations and central management systems.
- Attackers exploit input validation vulnerabilities in CMS communications over 3G/4G networks. They may use SQL injection, command injection, or other code injection techniques.

4.3 LAN(Local Area Network)

- Attackers can use weaknesses in services that allow remote access to systems, Once they're in, they exploit bugs or flaws in software or the operating system itself to run their own malicious code. Mitre Attack (Exploitation of Remote Services)
- Once attackers gain access to systems or accounts, they might send deceptive messages within the organization to steal more data or compromise other users. Specifically, high-stakeses Employees Mitre Attack (Internal Spearphishing).
- Attackers may take control of preexisting sessions with remote services to move laterally in an environment. They can use their login details to access services like telnet, SSH, or RDP, which allow remote connections to systems. Mitre Attack (Remote Service Session Hijacking)[14].

- BlueKeep (CVE-2019-0708) is a vulnerability in the Remote Desktop Protocol (RDP) on older Windows systems. Attackers can exploit it to execute remote code, create accounts, alter data, or install programs, all without user interaction [15].

4.4 Charging Management System (CMS)

- The OCPP backend does not properly restrict access to resources, allowing unauthorized actors to gain access. Attackers can exploit this weakness to gain elevated privileges, read restricted information, execute commands, or bypass security mechanisms. (CWE-284) [16].
- Attackers can perform man-in-the-middle (MitM) attacks to intercept and modify data between the EVCS and the backend. (CWE-923) [17].
- The OCPP backend does not limit the number of parallel connections from phantom EVCS using the same legitimate EVCS ID. Attackers can flood the backend with multiple connections from the same EVCS ID, overwhelming the system and causing a DoS [18].
- The OCPP backend relies solely on the EVCS ID for authentication, which is easily obtainable, making it easier for attackers to compromise systems. Attackers can easily obtain the EVCS ID and use it to authenticate and gain unauthorized access to the system.(CWE-654)[19].

4.5 Local Power Distribution Unit (Including SCADA)

- As SCADA protocols like DNP3 and Modbus do not employ encryption for data transmission. Attackers can intercept and modify data in transit, leading to unauthorized control or disruption of power distribution systems [20].
- SCADA systems often rely on simple authentication methods that can be easily bypassed. Allowing attackers to spoof authorized devices or gain administrative access to control panels.
- Power distribution systems often grow piece by piece, leading to tangled networks where SCADA systems might be poorly separated from corporate networks or internet, exposing them to security risks. Attackers who gain access to less secure parts of the network can pivot to target SCADA components.

- SCADA systems in power distribution often use specialized tech that lacks timely updates, leaving them vulnerable. Attackers can gain physical access to SCADA components, potentially leading to unauthorized control or disruption of power distribution[21].

4.6 Smart Meters

- Smart meters communicating over wireless network (3G/4G) may be vulnerable to eavesdropping if encryption is weak or absent. Attackers can monitor transmission patterns to infer information about power consumption and user presence[22].
- The CAT policy lets smart meters send data only after major power use changes, making communication patterns predictable. Attackers can exploit these predictable patterns to infer information about power consumption and user presence.
- Attackers with access to the firmware update mechanism could upload customized firmware containing malware. This could give them control, allowing them to manipulate readings or measurements[23].
- Attackers identify weak smart meters by analyzing network structures and intercepting unencrypted wireless communications. By using wireless sniffers or gaining physical access, they analyze data and security, then craft fake packets to alter meter readings[24].

5 Mitigation Strategies

5.1 Can Protocol

Attack Type	Mitigation Strategies
Sniffing Attacks (Eavesdropping)	Encrypt CAN messages (AES-128/256), use Secure CAN Protocols (CANsec, CAN FD Secure), implement Message Authentication Codes (MACs), segment the CAN network, disable debug ports on ECUs.
Frame Falsifying (Spoofing/Injection)	Use Message Authentication (HMAC, CMAC), implement sender-receiver pair authentication, whitelist valid CAN IDs, secure key management (HSM, TPM), use ML-based IDS for anomaly detection.
Denial-of-Service (DoS)	Implement rate limiting (throttle messages), use priority-based filtering, monitor bus load for excessive traffic, maintain redundant CAN channels, harden ECUs against message floods.
Bus-Off Attacks (ECU Isolation)	Implement auto-recovery policies, use watchdog timers for ECU resets, detect abnormal error frames, ensure redundant ECUs for critical tasks, secure boot & firmware updates.

Table 4: Mitigation Strategies for CAN Bus Attacks[25][26][27].

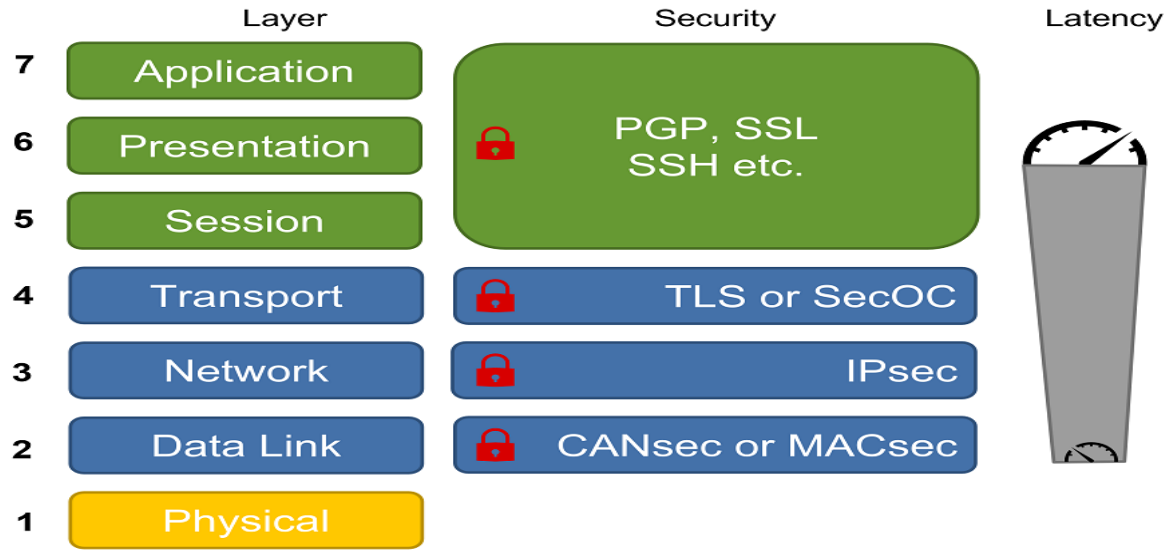


Figure 5: OSI Model Secured

5.2 3G/4G

Attack Type	Mitigation Strategies
MitM via Rogue Access Points / Compromised Networks	TLS 1.2/1.3 encryption for SCADA/EVCS communications, certificate pinning, network segmentation, IDS for rogue AP detection, MAC/port security on switches.
Weak Authentication in 3G/4G Backhaul	Multi-Factor Authentication (MFA), strong password policies (NIST SP 800-63B), IPsec VPNs over cellular networks, Zero Trust Architecture (ZTA).
Interception/Modification of Pricing Data	Blockchain-based integrity checks, digital signatures (ECDSA) for pricing updates, secure APIs (OAuth 2.0 + JWT) for CMS-EVCS communications.
Input Validation Exploits (SQLi/Command Injection)	Input sanitization (OWASP guidelines), Web Application Firewalls (WAFs) for CMS, least-privilege access control for database queries.

Table 5: Mitigation Strategies 3G/4G EVCS Security Threats[28][29][30].

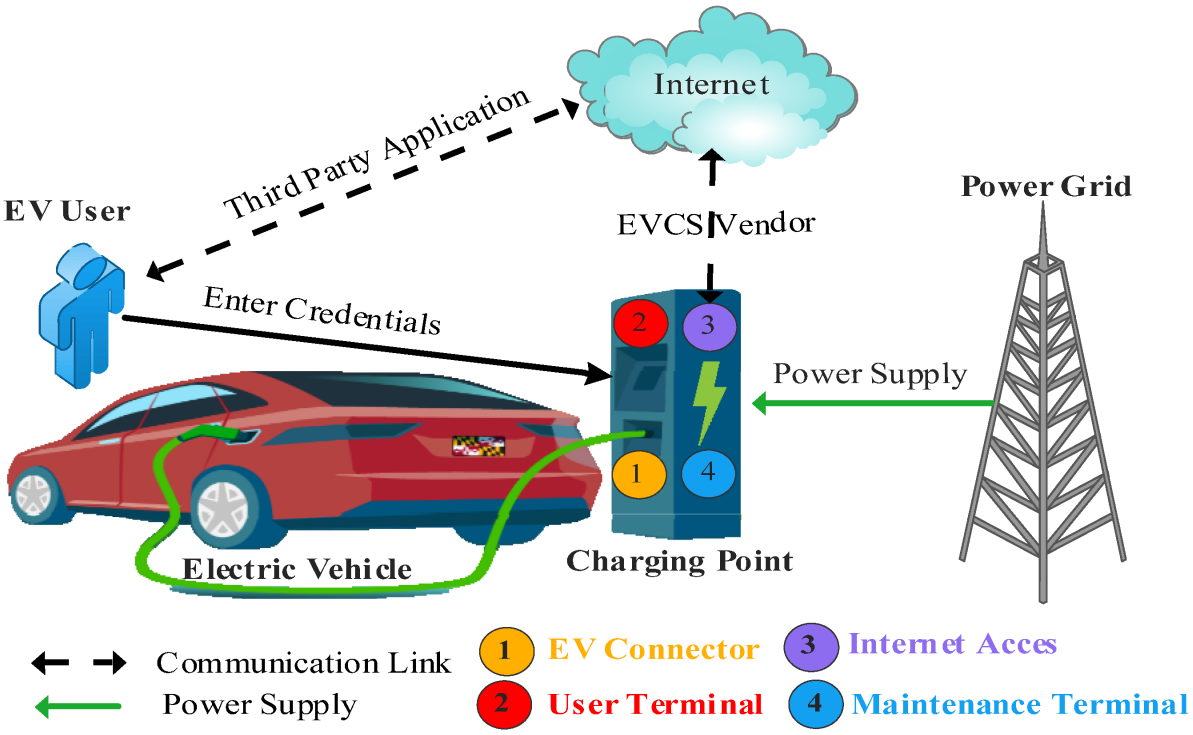


Figure 6: 3G/4G EV ecosystem

5.3 LAN(Local Area Network)

Attack Type	Mitigation Strategies
Exploitation of Remote Services (MITRE T1210)	Zero Trust Architecture (ZTA), regular patch management, network segmentation using IEC 62443, vulnerability scanning with Nessus/OpenVAS.
Internal Spearphishing (MITRE T1534)	Email/domain hardening (DMARC/DKIM/SPF), phishing simulations, behavioral analytics (UEBA tools).
Remote Service Session Hijacking (MITRE T1563)	MFA for remote access (FIDO2/TOTP), session encryption (SSHv2, disable Telnet), IP whitelisting with NAC solutions.
BlueKeep (CVE-2019-0708) Exploitation	Apply Microsoft's CVE-2019-0708 patch, disable RDP if unused, network segmentation via VLANs/firewalls.

Table 6: Mitigation Strategies for Remote Exploitation Threats[31][32][33][34].

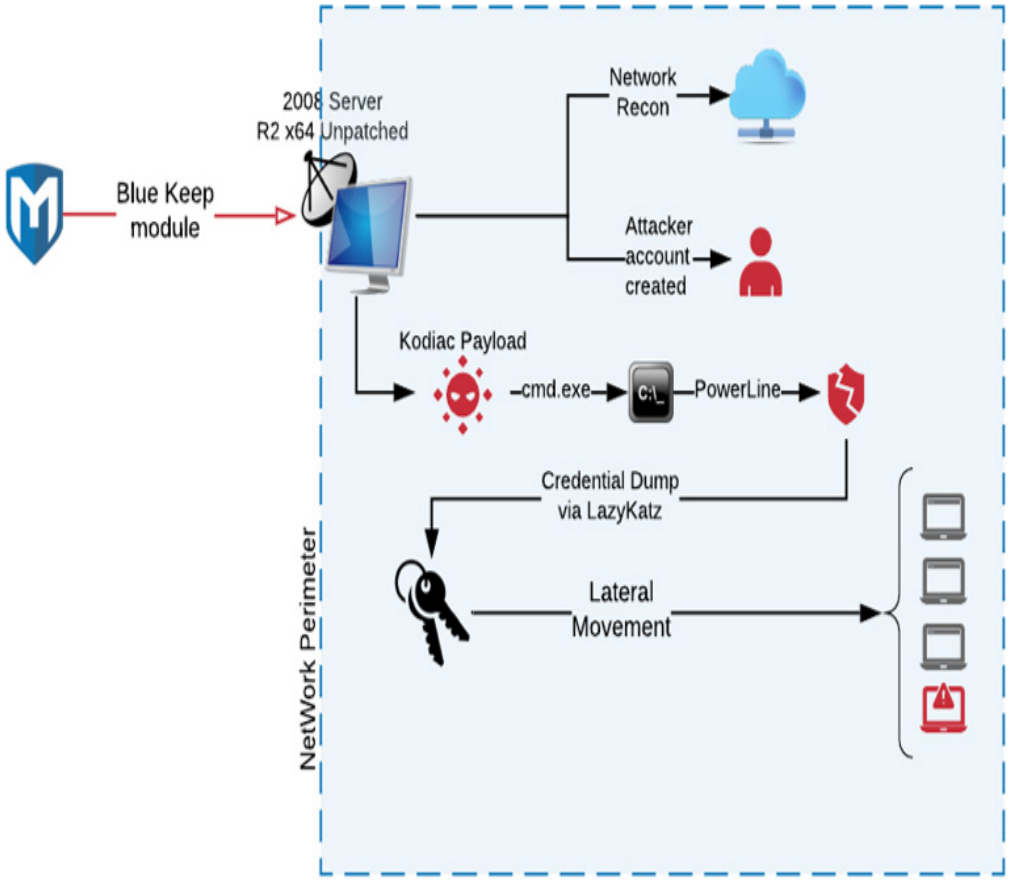


Figure 7: Bluekeep Exploit

5.4 Charging Management System (CMS)

Attack Type	Mitigation Strategies
CWE-284: Improper Access Control	Role-Based Access Control (RBAC) with fine-grained permissions, OpenID Connect (OIDC)/SAML, Zero Trust Architecture (NIST SP 800-207), OCPP-JSON/WebSocket validation.
CWE-923: MitM Attacks on OCPP Communications	TLS 1.3 encryption with mutual TLS (mTLS), certificate pinning, ECDSA/EdDSA for message integrity, IDS/IPS deployment for OCPP traffic.
Connection Flooding (DoS via Phantom EVCS)	Rate limiting (5 connections/IP), Kubernetes Ingress or NGINX enforcement, ML-based anomaly detection, unique session tokens per connection.
CWE-654: Weak EVCS ID Authentication	Multi-Factor Authentication (MFA) for EVCS registration, HSM/TPM for key storage, ISO 15118 Plug & Charge for cryptographic authentication.

Table 7: Mitigation Strategies for CMS[35][36][37].

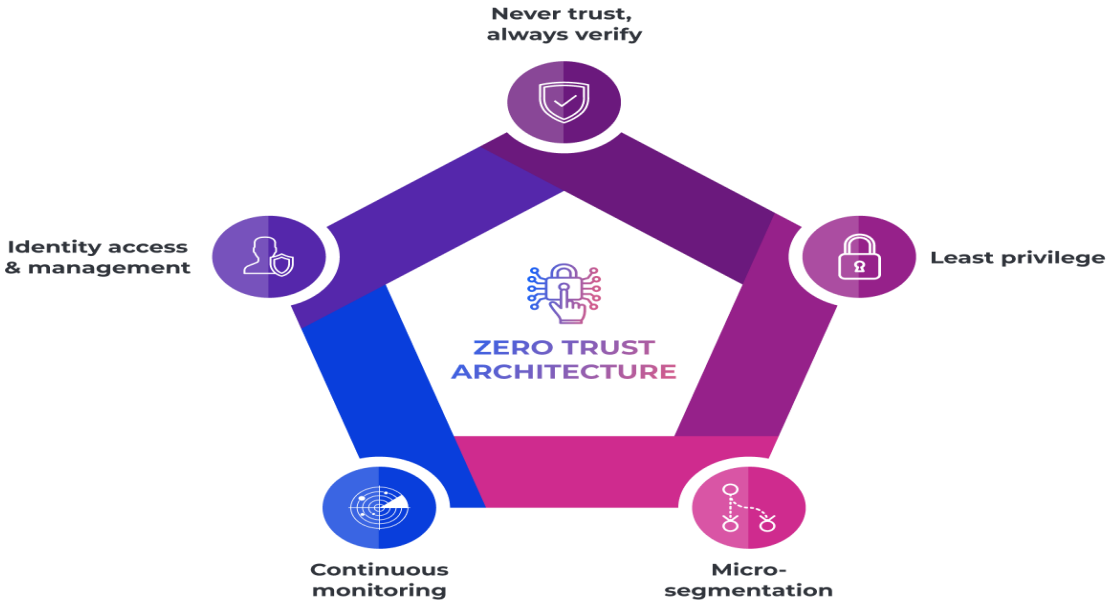


Figure 8: Zero Trust Architecture

5.5 Local Power Distribution Unit (Including SCADA)

Attack Type	Mitigation Strategies
Lack of Encryption in DNP3/Modbus (Interception/Modification)	Use DNP3 Secure Authentication (SAv5) with AES-256 (IEEE 1815-2012), Modbus/TCP with TLS, IPsec VPNs for RTU-control center connections, MACsec (IEEE 802.1AE) for LAN encryption.
Weak Authentication (Spoofing/Admin Access)	Implement X.509 certificates for RTU/PLC authentication (IEC 62351-3), use HSMs for key storage (FIPS 140-3), enforce MFA with smart cards + PINs.
Poor Network Segmentation (Lateral Movement)	Apply Zero Trust Architecture (ZTA) with microsegmentation (Tofino firewalls, Cisco ISA-3000), enforce Software-Defined Perimeters (NIST SP 800-207), use unidirectional gateways (e.g., Waterfall Security).
Outdated SCADA Firmware (Physical Access Risks)	Automate patch management (e.g., Siemens SINEC PDM), implement tamper-evident seals on RTUs/PLCs (NERC CIP-006), enforce Secure Boot + TPM 2.0 for firmware integrity.

Table 8: Mitigation Strategies for SCADA Security Threats[38][39]

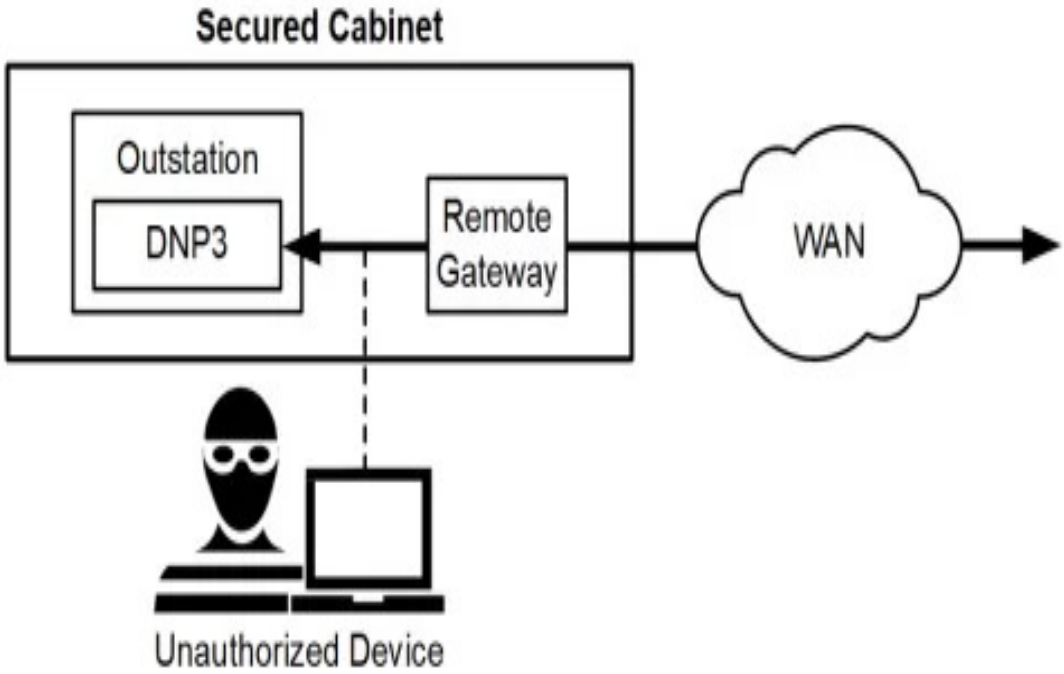


Figure 9: DNP3 Secure Protocol

5.6 Smart Meter Security

Threat	Mitigation Strategies
Eavesdropping via Weak/No Encryption	Use AES-128/256 encryption for smart meter communications (IEEE 802.15.4g), TLS 1.3 for backhaul (3G/4G) connections, and link-layer security (LoRaWAN AES-128).
Predictable Communication Patterns (CAT Policy)	Implement randomized reporting intervals, apply differential privacy for aggregated data (NIST IR 8278), and use Poisson-process-based transmissions to disrupt predictability.
Malicious Firmware Updates	Enforce code signing (ECDSA P-256), implement Secure Boot with TPM 2.0/HSM-based root of trust, and enable rollback protection against downgrade attacks.
Physical/Wireless Attacks (Sniffing/Spoofing)	Deploy RF shielding (Faraday cages), use wireless intrusion detection (Wireshark + custom plugins), and detect MAC spoofing via RSSI fingerprinting.

Table 9: Mitigation Strategies for Smart Meter Security Threats[40][41][42][43].

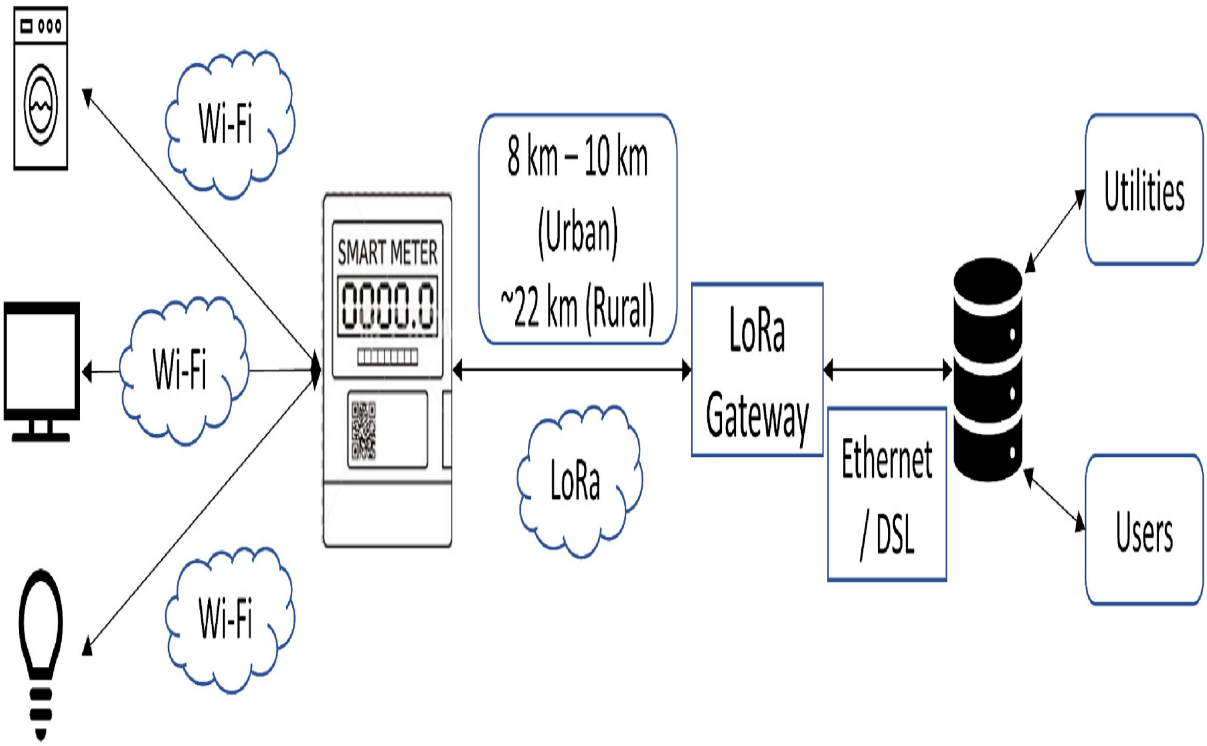


Figure 10: Smart meter using LoRaWan

6 Conclusion

The integration of EV charging with the smart grid introduces cybersecurity risks like unsecured protocols, outdated SCADA authentication, and vulnerable smart meter communication. Key defenses include encryption (AES-256, TLS 1.3), Zero Trust, multi-factor authentication, and AI-driven threat detection. Collaboration guided by standards like ISO 15118 and IEC 62351 is crucial to address these challenges.

7 Future Works

Focus on quantum-resistant cryptography, AI-driven threat detection, and blockchain-based OCPP authentication. Strengthen 5G-edge computing security and explore RF fingerprinting for device identification. Standardize OTA update frameworks, improve V2G resilience, and adapt defenses for renewable energy fluctuations. Promote human-centric training and foster collaboration to balance sustainability with robust cybersecurity.

References

[1] IEA (2024), Global EV Outlook 2024, IEA, Paris https://www.iea.org/reports/global-ev-outlook-2024, Licence: CC BY 4.0

[2] Electric vehicle attack impact on power grid operation Author Mohammad Ali Sayed , Ribal Atallah, Chadi Assi,

[3] Comprehensive Experimental Analyses of Automotive Attack Surfaces. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage.

[4] A Survey of Security Threats on 4G Networks. Yongsuk Park; Taejoon Park

[5] Managing cyber security vulnerabilities in large networks. Edward S. Chang; Aridaman K. Jain; David M. Slade; S. Lee Tsao

[6] Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles. Salah Adly ,Ahmed Moro ,Sherif Hammad and Shady A. Maged

[7] Transfer learning for securing electric vehicle charging infrastructure from cyber-physical attacks. Ahmad Almadhor, Shtwai Alsubai, Imen Bouazzi, Vincent Karovic, Monika Davidekova, Abdullah Al Hejaili & Gabriel Avelino Sampedro

[8] SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Manar Alanazi, Abdun Mahmood, Mohammad Jabed Morshed Chowdhury

[9] Uncovering Covert Attacks on EV Charging Infrastructure: How OCPP Backend Vulnerabilities Could Compromise Your System. Khaled Sarieddine, Mohammad Ali Sayed, Sadegh Torabi, Ribal Attallah, Danial Jafarigiv, Chadi Assi, Mourad Debbabi

[10] Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids. Husheng Li; Shuping Gong; Lifeng Lai; Zhu Han; Robert C. Qiu; Depeng Yang

[11] Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks. Abdullah, Muhammad Daniel Hafiz & Zurina, Mohd Hanapi & Zukarnain, Zuriati & Mohamed, Mohamad A.

[12] Microsoft Operating Systems BlueKeep Vulnerability. CISA.Gov

[13] CWE-284: Improper Access Control. Common Weak Enumeration

[14] Security Flaws Uncovered in EV Charging Infrastructure OCPP Backends. Alex Lekander

[15] CWE-654: Reliance on a Single Factor in a Security Decision. Common Weak Enumeration

[16] Attacking and Defending DNP3 ICS/SCADA Systems. Vasiliki Kelli, Panagiotis Radoglou Grammatikis

[17] Guide to Industrial Control Systems (ICS) Security. NIST.gov

[18] Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review. Nambundo, J.M.; de Souza Martins Gomes, O.; de Souza, A.D.; Machado,

[19] A small size planar MIMO LTE antenna system for USB dongle application. Shih-Chi Lai; Chi-Ming Jiang; Yi-Shin Chiou; Chia-Lun Tang

[20] Security aspects in Smart Meters: Analysis and Prevention. Rebeca P. Díaz Redondo, Ana Fernández Vilas and Gabriel Fernández dos Reis

[21] How hackers target smart meters to attack the grid. Yusuf Latief

[22] Secure communication over CANBus. Siddiqui, Ali Shuja & Gui, Yutian & Plusquellic, J. & Saqib, Fareena

[23] Practical Sender Authentication Scheme for In-Vehicle CAN With Efficient Key Management. Youn, Taek-Young & Lee, Yousik & Woo, Samuel

[24] The Art of Networking (Series 6): MACsec and CANsec – Layer 2 Security for High Performance Networks. Tobias Belitz

[25] Detecting and classifying man-in-the-middle attacks in the private area network of smart grids. Mohamed Faisal Elrawy, Lenos Hadjidemetriou, Christos Laoudias, Maria K. Michael

[26] Digital Identity Guidelines Authentication and Lifecycle Management. NIST.gov

[27] Secure Electric Vehicle Charging Infrastructure in Smart Cities: A Blockchain-Based Smart Contract Approach. Chowdhury, A.; Shafin, S.S.; Masum, S.; Kamruzzaman, J.; Dong, S.

[28] Zero Trust Architecture. NIST.gov

[29] Securing the Electric Vehicle Charging Infrastructure. Roberto Metere

[30] Theory and Application of Zero Trust Security: A Brief Survey. Hongzhaoning Kang, Gang Liu, Quan Wang, Lei Meng, Jing Liu

[31] SCADA security: a review and enhancement for DNP3 based systems. Peeyush Jain & Paritosh Tripathi

[32] Securing Over-the-Air Firmware Updates (FOTA) for Industrial Internet of Things (IIOT) Devices. Kenneth G. Crowther; Radhika Upadrashta; Gururaj Ramachandra

[33] Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator. Darshana Upadhyay,Sagarika Ghosh,Hiroyuki ,Marzia Zaman c, Srinivas Sampalli

[34] Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. Alomari, M.A.; Al-Andoli, M.N.; Ghaleb, M.; Thabit, R.; Alkawsi, G.; Alsayaydeh, J.A.J.; Gaid,

[35] Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256. Mehmet Adalier, Antara Teknik,

[36] Randomized Moving Target Approach for MAC-Layer Spoofing Detection and Prevention in IoT Systems. POORIA MADANI and NATALIJA VLAJIC,