IAES Journal of Electrical and Electronics Engineering
Vol. 11, No. 1, June 2024, pp. 6~10
ISSN: 2338-7432, DOI: 10.11591/jeee.v11i1.pp6-10

Cybersecurity and data privacy in smart electrical plug systems: a review of vulnerabilities, attack detection, and secure communication

Hany Safitry Febriningtyas[1], Tri Wahono[2], Anggit Pamungkas[2]
[1]Institute of Advanced Engineering and Science, Yogyakarta, Indonesia
[2]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia

Article Info

Article history:

Received Dec 24, 2021
Revised Apr 6, 2022
Accepted Jul 28, 2022

Keywords:

Authentication
Cybersecurity
Data privacy
Encryption
Internet of things
Intrusion detection
Smart electrical plugs

ABSTRACT

Smart electrical plugs are increasingly used to monitor energy consumption, automate appliances, and provide remote control through Internet of Things (IoT) platforms. However, their network connectivity and direct influence over electrical loads introduce cybersecurity and privacy risks that extend beyond conventional information leakage. This review examines vulnerabilities in smart plug architectures, focusing on insecure communication, weak authentication, firmware exposure, unauthorized access, and attacks against device availability and control. It also discusses how fine-grained electricity measurements can reveal household occupancy, routines, and appliance usage. Existing countermeasures are evaluated across device authentication, access control, encryption, secure communication protocols, privacy-preserving data processing, and intrusion detection. The review identifies a need to combine preventive security mechanisms with continuous monitoring and secure device lifecycle management. Particular attention is given to lightweight implementation because smart plugs operate with limited processing, memory, and energy resources. The findings indicate that layered protection, privacy-by-design, secure updates, and sustainable hardware practices should be integrated from the design stage to ensure reliable, safe, and trustworthy smart plug deployment.

This is an open access article under the CC BY-SA license.

1. INTRODUCTION

Smart electrical plugs have developed from simple remote switching devices into connected systems capable of measuring voltage, current, power, and energy consumption while communicating with mobile applications, cloud platforms, and home automation systems. Their convenience supports energy monitoring, appliance scheduling, and remote load management in residential, commercial, and laboratory environments. Nevertheless, network connectivity exposes these devices to unauthorized access, manipulation, and service disruption. Because a compromised smart plug can affect both digital information and the physical operation of an electrical appliance, its security requirements should include cybersecurity, privacy, and electrical safety [1], [2].

A significant research problem is that smart plugs may be deployed with limited processing capacity, inexpensive communication modules, and firmware that receives insufficient security maintenance. A direct investigation of commercial smart plug systems demonstrated practical weaknesses involving device scanning, brute-force attempts, spoofing, and firmware attacks [1]. These weaknesses can expose authentication credentials and enable unauthorized device control. Consequently, security cannot be treated as an optional software feature added after manufacturing, but should be incorporated into the complete device architecture [3], [4].

This review synthesizes research on smart plug vulnerabilities and related IoT security technologies published no later than 2023. It connects the principal risks to countermeasures involving network protection, authentication, encryption, privacy preservation, and attack detection. The review also considers sustainable

device design, particularly the need to maintain security over the operational lifetime of low-cost electronic products. Its central argument is that trustworthy smart plugs require coordinated protection across hardware, firmware, communication, cloud services, and user interaction.

2. SMART PLUG ARCHITECTURE AND SECURITY EXPOSURE

A typical smart plug consists of a metering circuit, microcontroller, switching element, communication interface, firmware, and an application or cloud service. These components form an interconnected architecture in which measurements are transmitted to external systems and control commands are returned to the device. Each interface creates a potential attack surface, including local wireless communication, cloud application programming interfaces, mobile applications, and firmware update mechanisms. General IoT security research emphasizes that vulnerabilities can emerge at the device, network, application, and service layers rather than from a single isolated component [2], [4], [5].

The security consequences are particularly important because smart plugs combine data collection with physical actuation. An attacker who gains control may switch appliances on or off, interfere with scheduled operation, or disrupt equipment connected to the outlet. Manipulated measurements may also mislead energy-management applications and compromise the reliability of consumption records. These risks make confidentiality, integrity, availability, authentication, and physical safety interconnected requirements rather than independent design objectives [1], [6].

3. MAJOR VULNERABILITIES AND CYBERATTACK SCENARIOS

Weak authentication is one of the most consequential vulnerabilities in connected plug systems. Default credentials, weak passwords, inadequate account recovery, and poorly protected device onboarding can allow unauthorized users to gain control. Brute-force attempts and credential reuse can further increase the likelihood of account compromise, especially when devices are accessible through internet-facing services. Research on IoT authentication demonstrates the importance of robust identity verification and secure key establishment for devices operating in heterogeneous networks [7].

Communication vulnerabilities create another major exposure because unprotected messages can be intercepted, modified, replayed, or impersonated. An attacker may attempt to capture control commands, impersonate a legitimate device, or manipulate messages between a plug and its cloud platform. Inadequate transport protection and insecure protocol configurations can expose both operational commands and consumption information. Reviews of IoT communication protocols and security threats therefore emphasize that protocol selection must be accompanied by correct authentication, encryption, and configuration [8].

Firmware and software weaknesses can provide persistent access to a compromised device. Outdated firmware, insecure boot procedures, insufficient update verification, and exposed debugging interfaces may allow attackers to modify device behavior or install malicious code. Denial-of-service attacks can also exhaust communication or processing resources, making remote monitoring and control unavailable. Broader IoT security studies identify insecure software, poor configuration, and inadequate lifecycle maintenance as recurring weaknesses across connected devices [3], [5].

Smart plug data also creates a distinct privacy problem because electricity consumption can reveal more than energy usage. Frequent measurements may indicate when occupants are present, when appliances are used, and how household activities change over time. Such information can be sensitive even when direct personal identifiers are removed, because consumption patterns may still be associated with particular users or households. Research on smart meter privacy demonstrates that energy data requires protection against inference and disclosure, making privacy-preserving collection and sharing relevant to smart plug applications [9], [10].

4. AUTHENTICATION, ENCRYPTION, AND SECURE COMMUNICATION

A secure smart plug should establish the identity of users, applications, gateways, and devices before accepting sensitive operations. Device onboarding should avoid universal default credentials and should use unique device identities supported by secure provisioning. Role-based or attribute-based access control can restrict users to the functions they are authorized to perform, such as monitoring consumption or switching a particular outlet. Research on IoT authentication and access control indicates that identity management and fine-grained authorization are essential for limiting unauthorized operations in interconnected environments [7], [11].

Encryption protects information while it is transmitted or stored, but it must be implemented together with integrity protection and secure key management. Transport layer security (TLS) can protect

communication between a smart plug, gateway, and cloud service, while datagram transport layer security (DTLS) may be appropriate for datagram-based constrained communication. Lightweight cryptographic techniques can reduce computational and memory overhead, but the selected algorithms must still provide appropriate security strength. The literature on IoT security and resource-constrained cryptography highlights the need to balance implementation cost, performance, and resistance to attack [4], [12].

Secure communication also requires protection against replay, impersonation, and unauthorized command execution. Each control message should be authenticated and should contain freshness information, such as a nonce, sequence number, or timestamp, to prevent previously captured commands from being reused. Secure update mechanisms should verify firmware authenticity and integrity before installation, while device credentials and cryptographic keys should be stored in protected memory whenever feasible. These measures are more effective when supported by secure boot, network segmentation, and a documented process for vulnerability disclosure and software maintenance [2], [8], [13].

5. CYBERATTACK DETECTION AND MONITORING

Preventive controls cannot guarantee that every attack will be blocked, making continuous monitoring an important part of smart plug security. Signature-based intrusion detection can identify known malicious traffic or recognized attack patterns, whereas anomaly-based detection can identify deviations from expected communication or device behavior. For smart plugs, useful indicators include repeated failed login attempts, unusual command frequency, unexpected changes in network destinations, abnormal data transmission, and switching events that conflict with authorized schedules. Research on IoT intrusion detection and smart home anomaly detection supports the use of network and behavioral features to identify suspicious activity [14], [15].

Machine learning can improve detection by identifying complex patterns that are difficult to describe through fixed rules. However, detection performance depends on representative datasets, realistic attack scenarios, and appropriate evaluation metrics. False alarms may interrupt legitimate appliance operation, while missed attacks may allow unauthorized control to continue undetected. Therefore, smart plug detection systems should be evaluated using detection rate, false-positive rate, response time, computational overhead, and communication cost rather than accuracy alone [14]-[16].

A practical architecture should combine local monitoring with gateway-level or cloud-assisted analysis. Local detection can respond quickly to suspicious switching commands or abnormal device behavior, while gateway monitoring can identify coordinated attacks involving multiple connected devices. Cloud analysis can support longer-term threat intelligence and model updates, provided that sensitive consumption data is minimized or protected. The smart home security literature also emphasizes that detection methods must account for diverse devices, changing user behavior, and the limited realism of some existing datasets [15], [16].

6. PRIVACY PROTECTION AND SUSTAINABLE DEVICE DESIGN

Privacy protection should begin by limiting the amount and granularity of data collected by a smart plug. High-frequency measurements should be retained only when they are necessary for a clearly defined function, while routine energy reports can use aggregated or reduced-resolution information. Access to detailed consumption histories should be restricted, and cloud services should communicate transparent retention and deletion policies. Privacy-preserving approaches discussed in smart metering research, including aggregation and noise-based techniques, offer relevant principles for reducing exposure in smart plug systems [9], [10].

Sustainable smart plug design should consider security across the entire product lifecycle rather than focusing only on initial energy efficiency. Durable components, replaceable or maintainable modules, low-power processing, and long-term firmware support can reduce electronic waste while improving security resilience. A device that becomes insecure because its manufacturer stops providing updates may need premature replacement, undermining its environmental benefits. Sustainable design should therefore include secure update capability, long-term support policies, repairability, and responsible end-of-life handling [3], [5].

Table 1 summarizes the principal threats and corresponding protection strategies for smart electrical plug systems. The comparison highlights that no single mechanism can address every vulnerability, because attacks may target the device, communication channel, user account, or consumption data. It also shows that privacy and sustainability should be considered alongside conventional network security. The table provides a practical basis for translating the reviewed research into design requirements.

Table 1. Cybersecurity and privacy threats and recommended countermeasures for smart electrical plugs

Threat or vulnerability	Potential consequence	Recommended countermeasure
Default or weak credentials	Unauthorized access and switching	Unique credentials, strong authentication, secure provisioning
Unencrypted communication	Data interception and command manipulation	TLS/DTLS, authenticated encryption, secure key management
Replay and spoofing attacks	Repeated or forged control commands	Nonces, sequence numbers, message authentication
Insecure firmware	Persistent compromise or malicious code	Secure boot, signed firmware, verified updates
Denial-of-service attacks	Loss of monitoring and remote control	Rate limiting, traffic monitoring, local fallback control
Excessive energy-data collection	Disclosure of occupancy and household routines	Data minimization, aggregation, retention limits
Unauthorized application access	Exposure or manipulation of device functions	Role-based access control and least privilege
Unsupported device software	Long-term exposure to known vulnerabilities	Lifecycle security support and maintainable design

7. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Despite progress in IoT cybersecurity, several research challenges remain for smart electrical plugs. First, many security studies address general IoT devices, while relatively few examine the combined cybersecurity and physical safety requirements of metering and switching outlets. Second, detection models require realistic datasets containing normal appliance operation, diverse household behavior, and multiple attack types. Third, security mechanisms must remain efficient enough for low-cost microcontrollers without compromising reliable switching or electrical protection [1], [14]-[18].

Future research should develop integrated security architectures that combine secure onboarding, lightweight cryptography, privacy-aware data management, and local anomaly detection. Standardized testing should measure not only communication security but also the effect of security mechanisms on switching latency, energy consumption, device availability, and fail-safe behavior. Manufacturers should also adopt transparent vulnerability reporting, signed firmware updates, and clearly defined support periods. These measures can strengthen trust while supporting sustainable and maintainable smart plug deployment [5], [7], [9], [12].

8. CONCLUSION

Cybersecurity and data privacy are fundamental requirements for smart electrical plug systems because these devices connect sensitive energy measurements with remotely controlled electrical loads. Existing research has demonstrated that weak authentication, insecure communication, firmware vulnerabilities, and insufficient access control can expose smart plugs to unauthorized access and manipulation. Consumption data also creates privacy risks because detailed electrical patterns may reveal household routines and occupancy. A reliable solution therefore requires layered protection that combines device authentication, encryption, secure key management, privacy-preserving data processing, and continuous attack detection. The review further indicates that security should be integrated with sustainable product design and long-term maintenance. Lightweight mechanisms are necessary for resource-constrained devices, but implementation efficiency must not weaken essential security properties or electrical safety. Secure boot, verified firmware updates, maintainable hardware, and long-term software support can reduce both cybersecurity exposure and premature electronic replacement. Ultimately, smart plugs should be designed as trustworthy cyber-physical devices in which security, privacy, reliability, and sustainability are addressed throughout the complete product lifecycle.

REFERENCES

[1] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: a case study of the smart plug system," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1899–1909, Dec. 2017, doi: 10.1109/JIOT.2017.2707465.
[2] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1–13, 2023, doi: 10.1016/j.iotcps.2022.12.003.
[3] M. Aqeel, F. Ali, M. W. Iqbal, T. A. Rana, M. Arif, and M. R. Auwul, "A review of security and privacy concerns in the internet of things (IoT)," *Journal of Sensors*, vol. 2022, pp. 1–20, Sep. 2022, doi: 10.1155/2022/5724168.
[4] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.
[5] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: a survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.
[6] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.

[7] A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," *Journal of Network and Computer Applications*, vol. 204, p. 103414, Aug. 2022, doi: 10.1016/j.jnca.2022.103414.
[8] A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Analysis on functionalities and security features of Internet of Things related protocols," *Wireless Networks*, vol. 28, no. 7, pp. 2857–2887, Oct. 2022, doi: 10.1007/s11276-022-02999-7.
[9] J. Kua, M. B. Hossain, I. Natgunanathan, and Y. Xiang, "Privacy preservation in smart meters: current status, challenges and future directions," *Sensors*, vol. 23, no. 7, p. 3697, Apr. 2023, doi: 10.3390/s23073697.
[10] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: a survey on security, privacy and open research issues," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019, doi: 10.1109/COMST.2019.2899354.
[11] R. Trabelsi, G. Fersi, and M. Jmaiel, "Access control in internet of things: a survey," *Computers and Security*, vol. 135, p. 103472, Dec. 2023, doi: 10.1016/j.cose.2023.103472.
[12] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained iot devices: a review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.
[13] N. Pattnaik, S. Li, and J. R. C. Nurse, "A survey of user perspectives on security and privacy in a home networking environment," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–38, Sep. 2023, doi: 10.1145/3558095.
[14] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair, and F. E. A. El-Samie, "Intrusion detection systems for the internet of thing: a survey study," *Wireless Personal Communications*, vol. 128, no. 4, pp. 2753–2778, Feb. 2023, doi: 10.1007/s11277-022-10069-6.
[15] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, "A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, Jan. 2023, doi: 10.1155/2023/8981988.
[16] J. I. I. Araya and H. Rifà-Pous, "Anomaly-based cyberattacks detection for smart homes: A systematic literature review," *Internet of Things*, vol. 22, p. 100792, Jul. 2023, doi: 10.1016/j.iot.2023.100792.
[17] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, "Survey on smart homes: vulnerabilities, risks, and countermeasures," *Computers and Security*, vol. 117, p. 102677, Jun. 2022, doi: 10.1016/j.cose.2022.102677.
[18] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.