RELIGACIÓN
REVISTA

Análisis de vulnerabilidades en medidores inteligentes y concentradores AMI: implicaciones de ciberseguridad y estrategias de protección

Analysis of vulnerabilities in smart meters and AMI concentrators: Cybersecurity implications and protection strategies

Carlos Santiago Tapia Chica, Diego Xavier Morales Jadán, Marcela Paz Sánchez Sarmiento, Juan Carlos Ortega Castro

Resumen:

La infraestructura de Medición Avanzada de Infraestructura (AMI) integra medidores inteligentes, redes de comunicación y sistemas de gestión de datos, facilitando una comunicación bidireccional entre las empresas de servicios públicos y sus clientes. Este sistema, que permite la recopilación y análisis detallado de datos de consumo energético, está en expansión debido a sus beneficios frente a los medidores tradicionales. Sin embargo, la gestión de grandes volúmenes de datos sensibles expone a la infraestructura AMI a amenazas significativas de ciberseguridad. Este artículo tiene como objetivo identificar las vulnerabilidades en los medidores inteligentes y los concentradores de datos de la red AMI, analizar las amenazas asociadas, evaluar las medidas de mitigación y examinar las posibles vulneraciones de derechos de los clientes. Se empleó el método PRISMA para revisar literatura relevante en bases de datos como Scopus y Web of Science. Los resultados muestran que tanto los medidores inteligentes como los concentradores de datos son vulnerables a ataques físicos y cibernéticos. Las estrategias de mitigación recomendadas incluyen la implementación de sellos de seguridad, autenticación y autorización de accesos, cifrado robusto de datos, actualizaciones periódicas de seguridad y autenticación de dispositivos para prevenir suplantaciones. Estas medidas son fundamentales para fortalecer la seguridad de la infraestructura AMI y proteger la integridad de los datos y derechos de los clientes.

Palabras clave: Vulnerabilidades AMI; Medidores inteligentes; Ciberseguridad; Mitigación de riesgos; Protección de datos.

Carlos Santiago Tapia Chica
Universidad Católica de Cuenca | Cuenca | Ecuador | carlos.tapia.41@est.ucacue.edu.ec
https://orcid.org/0009-0009-0535-950X
Diego Xavier Morales Jadán
Universidad Católica de Cuenca | Cuenca | Ecuador | dmoralesj@ucacue.edu.ec
https://orcid.org/0000-0002-4382-5219
Marcela Paz Sánchez Sarmiento
Universidad Católica de Cuenca | Cuenca | Ecuador | msanchezs@ucacue.edu.ec
https://orcid.org/0000-0002-8927-5478
Juan Carlos Ortega Castro
Universidad Católica de Cuenca | Cuenca | Ecuador | jcortegac@ucacue.edu.ec
https://orcid.org/ 0000-0001-6496-4325

http://doi.org/10.46652/rgn.v10i44.1311
ISSN 2477-9083
Vol. 10 No. 44 enero-marzo, 2025, e2501311
Quito, Ecuador

Enviado: agosto 05, 2024
Aceptado: septiembre 19, 2024
Publicado: octubre 13, 2024
Publicación Continua

Abstract

The Advanced Metering Infrastructure (AMI) integrates smart meters, communication networks, and data management systems, facilitating bidirectional communication between utility companies and their customers. This system, which enables detailed collection and analysis of energy consumption data, is expanding due to its advantages over traditional meters. However, managing large volumes of sensitive data exposes AMI infrastructure to significant cybersecurity threats. This article aims to identify vulnerabilities in smart meters and data concentrators within the AMI network, analyze associated threats, assess mitigation measures, and examine potential violations of customer rights. The PRISMA method was employed to review relevant literature in databases such as Scopus and Web of Science. Results indicate that both smart meters and data concentrators are vulnerable to physical and cyber attacks. Recommended mitigation strategies include the implementation of security seals, access authentication and authorization, robust data encryption, regular security updates, and device authentication to prevent impersonation. These measures are crucial for strengthening AMI infrastructure security and protecting data integrity and customer rights.

Keyword: AMI Vulnerabilities; Smart Meters; Cybersecurity; Risk Mitigation; Data Protection; Data Protection.

Introducción

La Infraestructura de Medición Avanzada (AMI) constituye un sistema integrado que abarca medidores inteligentes, redes de comunicación y sistemas de gestión de datos, facilitando la comunicación bidireccional entre las empresas de servicios públicos y los consumidores (ENERGY, 2016). Este sistema avanzado permite la recopilación y el análisis detallado de datos sobre el consumo energético, así como la ejecución de maniobras operativas sobre la infraestructura. Su implementación ha ido en aumento globalmente debido a las ventajas significativas que ofrece en comparación con los medidores tradicionales.

En el Centro de Investigación, Innovación y Transferencia Tecnológica (CIITT) de la Universidad Católica de Cuenca, se ha instalado una red AMI basada en tecnología de la marca HEXING para integrar un "Sistema de Medición Inteligente con el Simulador en Tiempo Real OPAL 5600" (Morales Jadán, 2022). Este sistema permite la obtención de señales eléctricas para el desarrollo de un programa de gestión de la demanda, la evaluación de los consumos energéticos y la creación de un entorno de prueba y simulación para la medición inteligente.

Sin embargo, la infraestructura AMI maneja una gran cantidad de datos sensibles y, dado que incluye componentes de comunicación, enfrenta inherentemente amenazas de ciberseguridad. Esta preocupación es relevante tanto para la seguridad de los sistemas AMI como para la protección de la información de los clientes, lo que representa un desafío significativo para las empresas de servicios públicos que implementan medidores inteligentes para la recopilación remota de datos de consumo energético (H. Kumar, 2023).

El objetivo de esta investigación es identificar y analizar las vulnerabilidades presentes en los medidores inteligentes y el concentrador de datos de la red AMI, evaluar las amenazas a las que están expuestos y desarrollar estrategias para mitigar dichos riesgos. Además, se busca entender las vulneraciones que afectan a los clientes finales de la red AMI mediante una revisión sistemática de la literatura existente.

Metodología

Para la metodología de este artículo, se aplicaron las directrices del método PRISMA (Page et al., 2021), el cual fundamenta su enfoque en la revisión sistemática de la literatura a través de bases de datos y artículos de libre acceso, como Web of Science y Scopus. Se establecieron tres preguntas clave para guiar la búsqueda de información, relacionadas con el objetivo de la investigación: las vulnerabilidades de los medidores inteligentes y el colector de datos en la red AMI, las recomendaciones para mitigar estas amenazas y las vulneraciones de derechos que afectan a los clientes. Se emplearon términos de búsqueda específicos, como "vulnerabilities of smart meter" y "vulnerabilities of collector AMI", para identificar documentos relevantes.

En la búsqueda inicial en Scopus, se recuperaron 304 documentos utilizando los scripts "vulnerabilities AND of AND smart AND meter" y "vulnerabilities of collector AMI". Posteriormente, se aplicaron criterios de filtrado para seleccionar documentación de los últimos dos años, con el fin de asegurar la actualidad de la información. Este proceso redujo el número de documentos a 88. De estos, se seleccionaron 21 que incluían los términos "detección" y "mitigación" de ciberataques en medidores inteligentes, los cuales fueron revisados detalladamente. La información revisada se presenta en la Tabla 1.

Tabla 1. Documentos obtenidos de Scopus.

Ítem	Titulo	Autores	Fuente	Año
1	Securing the green grid: A data anomaly detection method for mitigating cyberattacks on smart meter measurements	Farooq, Shahid, Olsen	International Journal of Critical Infrastructure Protection, 46, 100694	2024
2	A co-simulation environment to evaluate cyber resilience in active distribution grids utilising behind-the-meter assets	Hacker, Lenzen, Schmidtke, van der Velde, Ulbig	Electric Power Systems Research, 230, 110254	2024
3	"Hello? Is There Anybody in There?" Leakage Assessment of Differential Privacy Mechanisms in Smart Metering Infrastructure	Ghosh, Alam, Dey, Mukhopadhyay, D.	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 14585 LNCS, pp. 163–189	2024
4	A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security	Tatipatri, Arun	IEEE Access, 12, pp. 18147–18167	2024
5	Detecting smart meter false data attacks using hierarchical feature clustering and incentive weighted anomaly detection	Higgins, Stephen, Wallom,	IET Cyber-Physical Systems: Theory and Applications, 8(4), pp. 257–271	2023
6	An improved three-factor authentication and key agreement protocol for smart grid	Qi	Journal of Ambient Intelligence and Humanized Computing, 14(12), pp. 16465–16476	2023
7	When smart meters backfire on energy transition internalization: Ethical electricity suppliers' mitigation of consumer data vulnerability and attendant psychological disempowerment	Simon, Schweitzer	Technological Forecasting and Social Change, 194, 122738	2023

Ítem	Titulo	Autores	Fuente	Año
8	Smart meter vulnerability assessment under cyberattack events–An attempt to safeguard	Kumar, Raja Singh	Intelligent and Soft Computing Systems for Green Energy, pp. 79–95	2023
9	Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach	Awad, Shokry, Khalaf, Abd-Ellah	Computers and Electrical Engineering, 108, 108667	2023
10	Risk Assessment Method for 5G-oriented DLMS/COSEM Communications	Lekidis, Papageorgiou	2023 IEEE Conference on Standards for Communications and Networking, CSCN 2023, pp. 15–21	2023
11	Penetration Testing of Smart Meters against Cyber Attacks	Chaitanya, Aggarwal, Aggarwal, Kumar,	2023 IEEE Pune Section International Conference, PuneCon 2023	2023
12	Using Smart Meter Data to Predict and Identify Consumer Vulnerability	Wadsworth, Hodgins, Ellis, Troshka	IET Conference Proceedings, 2023(6), pp. 786–790	2023
13	Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks	Kumar, Alvarez, Kumar	IEEE Access, 11, pp. 55349–55360	2023
14	Data Privacy Preservation and Security in Smart Metering Systems	Abdalzaher, Fouda, Ibrahem	Energies, 15(19), 7419	2022
15	Hidden inequality in household electricity consumption: Measurement and determinants based on large-scale smart meter data	Chen, Zhang, Wang	China Economic Review, 71, 101739	2022
16	A Co-Simulation Environment to Evaluate Cyber Resilience in Active Distribution Grids Utilising Behind-the-Meter Assets	Hacker, Lenzen, Schmidtke, Van der Velde, Ulbig	IET Conference Proceedings, 2022(25), pp. 430–435	2022
17	An Evaluation of Cybersecurity Risks of DLMS/COSEM Smart Meter Using Fuzzing Testing	Wang, Shih, Liao, Chien	Proceedings–2022 IET International Conference on Engineering Technologies and Applications, IET-ICETA 2022	2022
18	Simulation and Analysis of Intrusion Resilient Smart Metering System	Patil, Acharya, Manthan, Nagasundari, Honnavalli	Lecture Notes in Electrical Engineering, 905, pp. 759–775	2022
19	A Review on Security and Privacy Issues in Smart Metering Infrastructure and Their Solutions in Perspective of Distribution Utilities	Yadav, Kumar	Lecture Notes in Electrical Engineering, 837, pp. 381–392	2022
20	Smart metering in EU and the energy theft problem	Gerasopoulos, Manousakis, Psomopoulos	Energy Efficiency, 15(1), 12	2022
21	Intrusion Resilience Analysis of Smart Meters	Sandhya, Nagasundari, Honnavalli	Lecture Notes in Electrical Engineering, 790, pp. 377–391	2022

Fuente: elaboración propia.

Realizando la búsqueda con los mismos criterios en Web of Science, se encontraron 88 documentos y aplicando criterios de filtrado para elegir documentación que contenga las palabas seguridad, medidor inteligente, análisis y prevención, se obtuvieron 4 documentos.

Tabla 2. Documentos obtenidos de Web of Science.

Ítem.	Titulo	Autores	Fuente	Año
1	Security Aspects in Smart Meters: Analysis and Prevention	Redondo, Fernández-Vilas and dos Reis	Jul 2020SENSORSarrow_drop_down 20 (14)	2014
2	Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks	Kumar, Alvarez and Kumar	2023IEEE ACCESSarrow_drop_down 11 , pp.55349-55360	2023
3	Data Privacy Preservation and Security in Smart Metering Systems	Abdalzaher, Fouda, and Ibrahem	Oct 2022ENERGIESarrow_drop_down 15 (19)	2022
4	Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision	Shokry, Awad, Khalaf	Nov 2022FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCEarrow_drop_down 136, pp.358-377	2022

Fuente: elaboración propia.

Resultados

En el análisis de vulnerabilidades de los medidores inteligentes y del concentrador de datos en la red AMI, se identificaron múltiples riesgos físicos y cibernéticos que afectan estos componentes críticos. La ubicación de los medidores inteligentes y concentradores de datos, a menudo en exteriores, los expone a ataques físicos y cibernéticos (Mostafa Shokry, 2022). Los accesos físicos no autorizados pueden permitir la manipulación directa de los equipos o sus componentes electrónicos, con el potencial de destruirlos, cortar cables de energía y comunicación, lo que interfiere con la transmisión y recepción de datos. Además, los medidores inteligentes están en riesgo de sufrir conexiones eléctricas ilegales, como "bypass", que pueden reducir o eliminar el registro del consumo de energía, así como sobrecargar los dispositivos para que se vuelvan inoperables.

También es posible que se acceda físicamente a puertos de comunicación, tales como USB, ópticos, ethernet o de programación. Este acceso puede facilitar ataques cibernéticos mediante la carga de software o firmware malicioso, o la extracción de datos. La instalación de dispositivos adicionales, como microcontroladores, puede interceptar y modificar los datos antes de que lleguen al sistema de gestión de datos. Los puertos de comunicación inalámbrica son especialmente vulnerables a interferencias o ataques que comprometen la seguridad si no se implementa un cifrado adecuado, permitiendo la manipulación remota de datos una vez establecido el acceso.

Además, el acceso web a los medidores inteligentes y a los concentradores puede ser objeto de ataques como inyecciones SQL, denegación de servicio (DoS) y denegación de servicio distribuido (DDoS). Estas vulnerabilidades pueden tener graves consecuencias, como la indisponibilidad del servicio eléctrico, fraudes en la facturación y el robo de información sensible de los clientes, como datos de consumo y detalles personales (Hägerling, 2014). Dado que AMI es un componente esencial para las "Smart grids", cualquier modificación no autorizada de los parámetros técnicos de

los medidores inteligentes puede alterar el estado de las redes eléctricas, provocando información errónea que afecta su funcionamiento.

El uso extendido de medidores inteligentes también plantea preocupaciones sobre la privacidad y seguridad (Gui Yutian, 2019). Los perfiles de carga de energía, que actúan como rasgos biométricos distintivos (Bicego, 2014), pueden ser utilizados para identificar individuos o grupos en función de sus patrones de consumo de energía (TUDOR, 2017), aumentando así las implicaciones sobre la privacidad personal.

En la mitigación de las vulnerabilidades identificadas en los medidores inteligentes y en el concentrador de datos de la red AMI, se pueden implementar varias estrategias para abordar tanto los riesgos físicos como los cibernéticos. Para contrarrestar los ataques físicos, se recomienda el uso de sellos de seguridad que permitan detectar manipulaciones no autorizadas, así como la instalación de placas de circuitería electrónica con protección anti-retiro. Además, es fundamental asegurar que los equipos se instalen en ubicaciones de alta seguridad para reducir el riesgo de acceso físico no autorizado.

En cuanto a la seguridad del acceso a los equipos, la implementación de mecanismos de autenticación y autorización es esencial para verificar la identidad de las entidades que se conectan a la red AMI, lo que ayuda a prevenir accesos no autorizados (Mostafa Shokry, 2022). Para preservar la confidencialidad de los datos y asegurar que la información intercambiada no quede expuesta, es recomendable utilizar técnicas avanzadas de cifrado de datos, como el cifrado simétrico o asimétrico (Khattak Asad, 2019; Muhammad, 2015).

Es crucial incorporar un cifrado robusto en los medidores inteligentes para proteger los datos energéticos tanto durante el tránsito como en su almacenamiento (Ajiboye, 2024). tecnologías de mejora de la privacidad (PET), tales como el cifrado de extremo a extremo, cifrado en reposo, anonimización y pseudonimización, deben ser implementadas para asegurar una protección adecuada de la información.

El mantenimiento de actualizaciones de seguridad proporcionadas por el fabricante es otra medida clave, dado que los medidores inteligentes y concentradores, al carecer de capacidad para ejecutar programas anti-malware por sí mismos, deben recibir actualizaciones periódicas para mantenerse protegidos (Seijo Simó Miguel, 2016).

Además, la infraestructura AMI debe contar con mecanismos de verificación de la legitimidad de los medidores inteligentes y concentradores de datos, asegurando su autenticación antes de integrarse a la red para evitar problemas de suplantación y permitir una monitorización efectiva de los componentes.

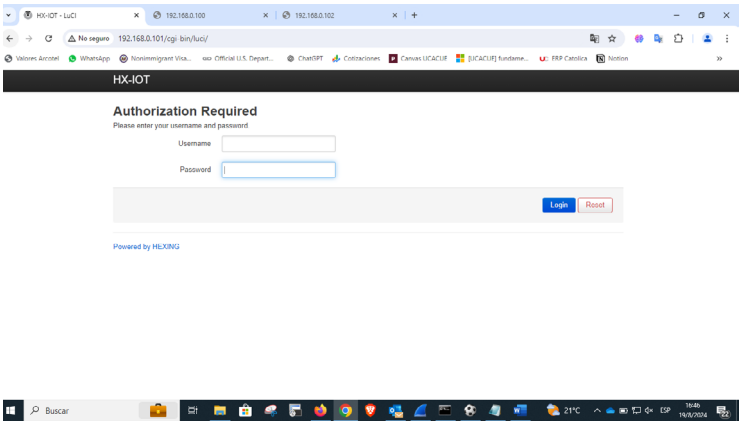
Se recomienda que las empresas de servicios públicos y los proveedores realicen ejercicios de seguridad regularmente, tales como pruebas de penetración y auditorías de seguridad, para

garantizar la integridad y robustez de los equipos antes de su recepción. Los medidores de marca Hexing, utilizados en el CIITT, emplean el estándar DLMS/COSEM, que proporciona mecanismos de seguridad adicionales, incluyendo autenticación y cifrado (Butun, 2022).

En relación con la vulneración de derechos de los clientes, es crucial reconocer el riesgo de violaciones a la privacidad y seguridad de los datos personales. La recopilación de información sobre el consumo de energía, junto con datos personales, puede revelar detalles sensibles en caso de un ataque de ciberseguridad. La exposición de esta información comprometería aspectos del estilo de vida de los usuarios y sus patrones de uso de la energía, lo que subraya la importancia de proteger estos datos para evitar la revelación de información privada.

Para el análisis de vulnerabilidades en la red como prueba piloto, se utilizó la herramienta Wireshark para mapear el direccionamiento de la red y detectar los dispositivos que transmitían paquetes. Esta fase inicial permitió identificar la IP 192.168.0.101 como perteneciente al concentrador de datos de la marca Hexing, instalado en el laboratorio. La comunicación con este dispositivo fue verificada exitosamente mediante la conexión a través de un navegador web, lo que permitió confirmar la accesibilidad y operatividad del concentrador dentro de la red de pruebas, ver figura 1.

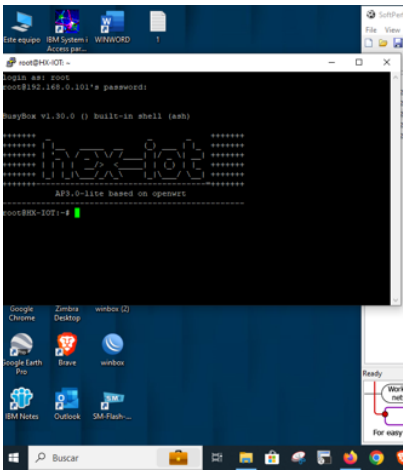
Figura 1. Acceso web del concentrador de datos AMI bajo la IP: 192.168.0.101.



Fuente: producción propia.

Se llevó a cabo un ataque de fuerza bruta para probar la seguridad de las credenciales de acceso del concentrador de datos. Tras obtener acceso al sistema, se pudo extraer la configuración completa del dispositivo. Además, se verificó que el puerto 22 (SSH) estaba abierto, lo que facilitó el acceso al concentrador mediante este protocolo, permitiendo así una administración más profunda y potencialmente peligrosa del equipo sin necesidad de usar la interfaz web, ver figura 2.

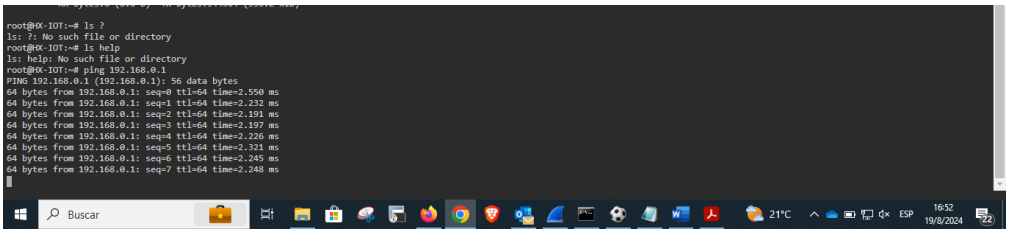
Figura 2. Acceso mediante ssh al concentrador de datos.



Fuente: producción propia.

Asimismo, se accedió a las configuraciones avanzadas, incluyendo la pantalla de actualización de firmware, lo que subraya las vulnerabilidades presentes en el sistema. Las pruebas de ping realizadas desde el concentrador de datos hacia el router confirmaron una comunicación constante y sin interrupciones entre estos equipos, lo cual podría ser explotado por un atacante para mantener una presencia persistente en la red, como se observa en la figura 3.

Figura 3. Prueba de ping desde el concentrador de datos hacia el router de la red.



Fuente: producción propia.

Discusión

Ante las vulnerabilidades detectadas, se propone implementar contraseñas robustas para el equipo concentrador de datos Hexing. Estas contraseñas deben incluir una combinación de caracteres especiales, números, y letras mayúsculas y minúsculas para aumentar la complejidad y reducir la posibilidad de ataques de fuerza bruta. Además, es crucial configurar una "Access List" en el router TPlink EC225-G5, que limite el acceso únicamente a usuarios autorizados, previniendo que usuarios no autorizados puedan interactuar con la red y, por ende, con el concentrador de datos.

Se recomienda deshabilitar el acceso al concentrador de datos a través de un navegador web, permitiendo únicamente la conexión mediante SSH. Esto dificultaría la explotación de

vulnerabilidades que puedan ser más fácilmente accesibles a través de interfaces web. Asimismo, se sugiere la inversión en un router con capacidades avanzadas de control de puertos, que permita habilitar únicamente los puertos necesarios para la operación del concentrador de datos, minimizando el riesgo de acceso no autorizado a la red.

Implementar VLANs para segmentar la red es otra estrategia clave, permitiendo la separación de rutas de modo que el acceso a la gestión de los equipos AMI esté aislado de otros servicios de red como internet, intranet y telefonía. Esta segmentación aumenta la seguridad al dificultar la propagación de amenazas entre diferentes segmentos de la red. Finalmente, se recomienda que el router esté integrado con un firewall para controlar el acceso al concentrador de datos, ofreciendo así una capa adicional de seguridad mediante el monitoreo y filtrado del tráfico hacia el concentrador, y previniendo accesos no autorizados.

Conclusión

En conclusión, los ciberataques a la infraestructura de Medición Avanzada de Infraestructura (AMI) presentan una amenaza significativa que puede ser atribuida a una variedad de actores, incluidos empleados descontentos, consumidores, proveedores, agencias de inteligencia extranjeras, competidores, organizaciones criminales, terroristas e incluso extorsionadores.

Los objetivos de estos ataques son diversos y van desde la interrupción remota del suministro eléctrico a usuarios, grupos o industrias, hasta la desactivación de medidores para impedir la recolección de datos por parte de los operadores de red. Además, la captura de datos de los medidores con fines de venta para obtener beneficios económicos también representa un riesgo considerable.

Estos ciberataques no solo tienen el potencial de causar pérdidas financieras significativas a las empresas de servicios públicos, sino que también comprometen la confiabilidad de la red eléctrica. La integridad y precisión de los datos recogidos por los medidores inteligentes son cruciales para una gestión eficiente y efectiva de la red eléctrica. La manipulación o pérdida de estos datos puede afectar la capacidad de las empresas para gestionar la red, optimizar el suministro eléctrico y proporcionar un servicio fiable a los consumidores.

Las estrategias de mitigación identificadas, como el uso de cifrado robusto, autenticación multifactor, y la implementación de medidas físicas de seguridad, ofrecen una base sólida para abordar las vulnerabilidades existentes. Sin embargo, es esencial que las empresas de servicios públicos y proveedores de tecnología continúen desarrollando e implementando soluciones innovadoras y adaptativas para enfrentar las amenazas emergentes.

La colaboración entre la industria, investigadores y reguladores será clave para fortalecer la seguridad de las redes AMI, proteger la infraestructura crítica y asegurar la confianza del consumidor en el contexto de una infraestructura eléctrica moderna y cada vez más interconectada.

Referencias

Ajiboye P.O. (2024). Privacy and security of advanced metering infrastructure (AMI) data and network: a comprehensive review. *Journal of Engineering and Applied Science, 71*(1).

Bicego, F. R. (2014). *Behavioural biometrics using electricity load profiles. In Pattern Recognition (ICPR)* [Conferencia]. 22nd International Conference on IEEE.

Butun, I. L. (2022). *Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities.* Science and Technology Publications, Ltda.

ENERGY, U. D. (2016). *Advanced Metering Infraestructure and Customer Systems.*

Hägerling, F. K. (2014). *Communication architecture for monitoring and control of power distribution grids over heterogeneous ICT networks* [Conferencia]. IEEE International Energy Conference (ENERGYCON).

Kumar, O. A. (2023). Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks. *IEEE Access,* 11, 55349-55360.

Khattak Asad, K. S. (2019). *Smart Meter Security: Vulnerabilities, Threat Impacts, and Countermeasures.* Springer.

Gui Yutian, S. A. (2019). *Security Vulnerabilities of Smart Meters in Smart Grid* [Conferencia]. IECON 2019–45th Annual Conference of the IEEE Industrial Electronics Society.

Morales Jadán, D. X. (2022). *Sistema de medición inteligente integrada al simulador en tiempo real.* OPAL.

Mostafa Shokry, A. I.-E. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Generation Computer Systems,* 136, 358-377.

Muhammad Daniel Hafiz Abdullah, Z. M. (2015). Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks. *KSII Transactions on Internet and Information Systems,* 9, 1493-1515.

Page M J, M. J. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ,* (71).

Seijo Simó Miguel, L. G. (2016). *El reto de la ciberseguridad en infraestructuras de medición avanzada* [Conferencia]. III Congreso de Smart Grids. https://lc.cx/Nz_iSf

Tudor, V. (2017). Enhancing *Privacy in the Advanced Metering Infrastructure: Efficient Methods, the Role of Data Characteristics and Applications* [Tesis de doctorado, Chalmers University of Technology].

Autores

Carlos Santiago Tapia Chica. Ingeniero Electrónico, estudiante del máster de Ciberseguridad de la Universidad Católica de Cuenca.

Diego Xavier Morales Jadán. Profesor e investigador de la Universidad Católica de Cuenca.

Marcela Paz Sánchez Sarmiento. Profesora e investigadora de la Universidad Católica de Cuenca.

Juan Carlos Ortega Castro. Profesor e investigador de la Universidad Católica de Cuenca.

Declaración

Conflicto de interés
No tenemos ningún conflicto de interés que declarar.
Financiamiento
Sin ayuda financiera de partes externas a este artículo.
Nota
Este artículo es realizado como parte del proceso de titulación de posgrado.