RELIGACIÓN
REVISTA

Seguridad en redes de medición avanzada (AMI): amenazas, mitigación y estrategias en el contexto de Smart Grids

Security in advanced metering networks (AMI): Threats, mitigation and strategies in the context of Smart Grids

Jason Roberto Bermeo Varela, Diego Xavier Morales Jadán, Marcela Paz Sánchez Sarmiento, Manuel Salvador Álvarez Vera

Resumen:

Las redes eléctricas inteligentes, o Smart Grids, han revolucionado el sector eléctrico mediante soluciones innovadoras en generación, transmisión y distribución; sin embargo, la seguridad en la cadena final conectada al consumidor ha sido históricamente desatendida. Este artículo analiza las amenazas de seguridad en las redes de Medición Avanzada de Infraestructura (AMI) y propone estrategias de mitigación para garantizar su integridad y confiabilidad. Los objetivos son identificar y analizar las amenazas de seguridad en las redes AMI, evaluar su impacto potencial y discutir estrategias actuales para mitigar los riesgos asociados, proporcionando recomendaciones para mejorar la seguridad de estas redes en el contexto de la medición eléctrica inteligente. La metodología incluyó una revisión exhaustiva de la literatura existente sobre seguridad en redes AMI, identificación de amenazas como ataques cibernéticos, intrusiones físicas y vulnerabilidades en la comunicación, evaluación del impacto potencial de estas amenazas y desarrollo de propuestas de mejora basadas en mejores prácticas y tecnologías emergentes. El análisis reveló amenazas significativas como Tampering, acceso no autorizado, ataques de denegación de servicio (DoS), inyección de comandos y sniffing. Las estrategias de mitigación identificadas incluyen cifrado avanzado, mecanismos de autenticación fuertes, monitoreo continuo de la red y medidas físicas de seguridad. La seguridad en las redes AMI es crucial para la operación segura y fiable de las redes eléctricas inteligentes, destacando la necesidad de enfoques multidisciplinarios. Las tecnologías y estrategias actuales son efectivas, pero es esencial continuar desarrollando soluciones innovadoras y adaptativas para enfrentar las amenazas emergentes. La implementación de prácticas de seguridad robustas no solo protegerá la infraestructura eléctrica, sino que también fomentará la confianza del consumidor y mejorará la resiliencia de las redes inteligentes frente a posibles ataques.

Palabras clave: Ciberseguridad; Redes AMI; Smart Grids; Vulnerabilidades; Estrategias de mitigación.

Jason Roberto Bermeo Varela
Universidad Católica de Cuenca | Cuenca | Ecuador | jason.bermeo@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
Manuel Salvador Álvarez Vera
Universidad Católica de Cuenca | Cuenca | Ecuador | malvarezv@ucacue.edu.ec
https://orcid.org/0000-0002-2521-0042

http://doi.org/10.46652/rgn.v10i44.1312
ISSN 2477-9083
Vol. 10 No. 44 enero-marzo, 2025, e2501312
Quito, Ecuador

Enviado: agosto 05, 2024
Aceptado: septiembre 19, 2024
Publicado: octubre 14, 2024
Publicación Continua

RELIGACIÓN CICSHAL
Centro de Investigaciones en Ciencias Sociales y Humanidades desde América Latina

Abstract

Smart grids have revolutionized the electric sector with innovative solutions in generation, transmission, and distribution; however, the security of the final consumer-connected chain has historically been neglected. This article analyzes security threats in Advanced Metering Infrastructure (AMI) networks and proposes mitigation strategies to ensure their integrity and reliability. The objectives are to identify and analyze security threats in AMI networks, evaluate their potential impact, and discuss current strategies to mitigate associated risks, providing recommendations to enhance the security of these networks within the context of smart metering. The methodology included a comprehensive review of existing literature on AMI network security, identification of threats such as cyber-attacks, physical intrusions, and communication vulnerabilities, assessment of the potential impact of these threats, and development of improvement proposals based on best practices and emerging technologies. The analysis revealed significant threats such as tampering, unauthorized access, denial of service (DoS) attacks, command injection, and sniffing. Identified mitigation strategies include advanced encryption, strong authentication mechanisms, continuous network monitoring, and physical security measures. Security in AMI networks is crucial for the safe and reliable operation of smart grids, highlighting the need for multidisciplinary approaches. Current technologies and strategies are effective, but it is essential to continue developing innovative and adaptive solutions to address emerging threats. Implementing robust security practices will not only protect the electrical infrastructure but also foster consumer trust and improve the resilience of smart grids against potential attacks.

Keyword: Cybersecurity; AMI Networks; Smart Grids; Vulnerabilities; Mitigation Strategies.

Introducción

La implementación de medición inteligente en puntos estratégicos de la red de bajo voltaje permite la recepción en tiempo real de variables eléctricas clave como voltaje, corriente y potencia. Un monitoreo adecuado de estas variables facilita la toma de acciones de control, incluyendo el envío de comandos de corte y conexión, así como la recepción de alarmas operativas. En este contexto, la seguridad es fundamental para garantizar el correcto funcionamiento, considerando que los equipos pueden estar desplegados en diversos ambientes y localidades.

Con el crecimiento exponencial de la tecnología y la inteligencia artificial, las vulnerabilidades potenciales se vuelven cada vez más accesibles para ser explotadas. En este contexto, el objetivo de este artículo es identificar y analizar las principales amenazas de seguridad en las redes AMI (Infraestructura de Medición Avanzada), evaluar el impacto potencial de estas amenazas y discutir las estrategias y tecnologías actuales para mitigar los riesgos asociados. Además, se pretende proporcionar recomendaciones para mejorar la seguridad de las redes AMI en el contexto de la medición eléctrica inteligente.

Los estudios sobre la gestión de la demanda de energía eléctrica mediante una medición inteligente adecuada son imprescindibles en la cadena de suministro y en los esquemas de mercados eléctricos a nivel mundial. Los avances en redes inteligentes, la gestión descoordinada del consumidor final, las mediciones en tiempo real y las nuevas fuentes de generación no son suficientes para una gestión activa de la demanda. El consumidor, en muchos casos, no se involucra con el uso final de la energía ni integra sus procesos industriales y comerciales, sin conocer el potencial de reducción de costos que esto podría representar (Al-Soud & Hrayshat, 2004).

Esta investigación permitirá integrar recursos energéticos de grandes consumidores en un escenario de red inteligente, incluyendo el potencial abastecimiento proporcionado por las plantas virtuales de energía (VPP, por sus siglas en inglés), bajo la administración de un agregador. Se analizarán los riesgos y vulnerabilidades en las implementaciones de lectura inteligente de las redes AMI, siguiendo lineamientos de estándares de representación y considerando el entorno de despliegue (Garcia & Lee, 2018).

Adicionalmente, este beneficio se refleja en la gestión administrativa de las empresas, que, con la implementación de planes y programas de mejora continua, podrían captar nuevos mercados gracias a la calidad, precio y beneficios ofrecidos. La investigación propone una metodología para el diseño eléctrico y de telecomunicaciones de la arquitectura necesaria para realizar la medición, sirviendo como guía tanto para las empresas como para los usuarios que buscan innovaciones tecnológicas en el recurso energético de primera necesidad.

Las ciudades, como sistemas complejos, requieren una relación constante entre población y tecnología para mantener un ecosistema sostenible. Esto incluye propuestas de electromovilidad, ciudades inteligentes y servicios de tecnologías de la información y el conocimiento (Ehrler & Hebes, 2012). La incorporación de tecnologías para la cuantificación de los flujos eléctricos permite una visualización clara del consumo de energía, tanto general como específico, en los procesos de transporte, distribución y comercialización del flujo eléctrico.

La medición avanzada es una herramienta que genera información basada en el monitoreo permanente de parámetros eléctricos y la transferencia de esta información a los centros de control. Entre los beneficios se encuentra la capacidad de mostrar, de manera precisa, los detalles de consumo de los usuarios y los diferentes nodos de la red, lo cual es útil para balances de energía y la identificación de pérdidas técnicas y no técnicas (Meneses Ruiz, 2016).

Los dispositivos utilizados en las redes AMI cuentan con tres posibles canales de comunicación: puerto ethernet para conexión cableada (LAN), módulo de red inalámbrica (WiFi) y GPRS para registro de datos mediante red celular, asegurando la integridad de la información con cifrado adecuado. Sin embargo, un estudio detallado por Fovino (2011), del Instituto para la Protección y la Seguridad de los Ciudadanos (IPSC) ha identificado varias vulnerabilidades de seguridad en los protocolos de comunicación SCADA, especialmente en equipos obsoletos y sistemas operativos desactualizados, lo que los convierte en objetivos fáciles de vulnerar (Arciniegas et al., 2017).

En cuanto a la infraestructura eléctrica, existen múltiples riesgos cibernéticos, desde proveedores y clientes hasta organizaciones de crimen organizado y terroristas. Estos riesgos incluyen cortes de servicio, captura de datos con fines maliciosos, denegación de servicios y vulneración de datos para fines económicos. Según la investigación "Data Analysis with Smart Measurement AMI", las redes AMI presentan un promedio de 4,6% de pérdida de datos durante la comunicación, lo que refleja posibles riesgos de pérdida de datos y/o denegación del servicio (National Institute of Standards and Technology, 2010).

El análisis de tecnologías y la revisión bibliográfica sobre seguridades en redes AMI, junto con los lineamientos del documento NIST para ciberseguridad en redes inteligentes, destacan varias vulnerabilidades:

1. Manipulación de Datos (Tampering): Protección de la confidencialidad de la información.
2. Acceso No Autorizado: Identificación y autenticación de usuarios.
3. Ataques de Negación de Servicio (DoS): Mitigación de los efectos de ataques DoS.I
4. Inyección de Comandos: Prevención de inyección de comandos maliciosos.
5. Falta de Cifrado (Sniffing): Protección de la integridad de la información.
6. Protección Perimetral: Definición de las fronteras del sistema.

Metodología

La investigación presentada en este artículo se caracterizó por su naturaleza descriptiva, justificada por varios motivos fundamentales. En primer lugar, se llevó a cabo una revisión bibliográfica, basada en una evaluación detallada de la literatura existente, incluyendo artículos científicos, informes técnicos y estándares de la industria. Este enfoque permitió describir y documentar de manera sistemática las amenazas y vulnerabilidades presentes en las redes AMI, así como las estrategias actuales para su mitigación.

Se identificaron y clasificaron las principales amenazas de seguridad que afectan a las redes AMI. Este proceso incluyó la descripción de diferentes tipos de ataques y vulnerabilidades, proporcionando una comprensión clara y detallada de los riesgos asociados. La evaluación del impacto potencial de estas amenazas en la operación y la integridad de las redes AMI se realizó mediante la descripción de escenarios hipotéticos y análisis cualitativos, ilustrando cómo diversas amenazas podrían afectar el funcionamiento de las redes y la recolección de datos.

Se efectuó un análisis descriptivo de las tecnologías y prácticas empleadas para mitigar los riesgos de seguridad en las redes AMI. Este análisis abarcó la descripción de mecanismos de cifrado, autenticación, detección de intrusiones y medidas físicas de seguridad. Las recomendaciones propuestas se basaron en una descripción detallada de las mejores prácticas y tecnologías emergentes, proporcionando un marco de referencia para la implementación de medidas de seguridad más robustas en las redes AMI.

Como fuentes de información primaria se utilizaron estudios que abordaran la ciberseguridad en redes eléctricas inteligentes con AMI, publicados en inglés, entre 2010 y 2024, y disponibles en texto completo. Se excluyeron estudios que no abordaran específicamente la ciberseguridad, trabajos duplicados, resúmenes de conferencias y estudios no revisados por pares. Los datos se sintetizaron utilizando un enfoque narrativo y cualitativo, y se realizó un meta-análisis cuando fue

apropiado para combinar los resultados cuantitativos de estudios similares.

Sobre la red AMI, la investigación se centró en identificar y mitigar vulnerabilidades en una infraestructura avanzada de medición (AMI) mediante pruebas prácticas en un entorno controlado. Se configuró una red AMI simulada, que incluía medidores inteligentes, un concentrador de datos Hexing, un router TPLink y un dispositivo atacante simulado.

Se utilizó Wireshark para capturar y analizar el tráfico de red, identificando direcciones IP clave y puntos de vulnerabilidad, como la exposición del puerto SSH en el concentrador de datos, lo que permitió acceder al servicio SSH y evaluar la seguridad de las credenciales y configuraciones de firmware.

A partir de estos hallazgos, se realizaron pruebas de conectividad y se formularon recomendaciones de seguridad para fortalecer la red AMI. Estas incluyeron el uso de contraseñas más robustas, la implementación de listas de control de acceso, la restricción del acceso mediante SSH y la segmentación de la red con VLANs. La metodología utilizada no solo permitió identificar vulnerabilidades críticas, sino que también facilitó la propuesta de medidas concretas para mejorar la ciberseguridad en infraestructuras de medición avanzada

Resultados

Como caso de estudio, se trabajó sobre la red AMI del sistema de medición inteligente integrada al simulador en tiempo real OPAL 5600, en la Universidad Católica de Cuenca, las amenazas identificadas incluyeron ataques de intercepción y manipulación de datos. Se observó que la transmisión de datos en las redes AMI, cuando no está adecuadamente cifrada, es vulnerable a interceptaciones y manipulaciones. Los atacantes pueden acceder a la información de consumo energético y alterar los datos para provocar errores en la facturación o el control de la red.

Asimismo, las intrusiones físicas fueron una preocupación, ya que los dispositivos AMI, como los medidores inteligentes, están expuestos a manipulaciones físicas que pueden permitir el acceso no autorizado. Estas intrusiones pueden resultar en la alteración de los datos de medición o el sabotaje de la red.

Otra amenaza significativa identificada fueron los ataques de denegación de servicio (DoS). Las redes AMI son susceptibles a estos ataques que pueden interrumpir la comunicación entre los dispositivos y los sistemas centrales, llevando a la pérdida de datos, la interrupción del servicio y la imposibilidad de monitorear y controlar la red en tiempo real. Además, se identificaron varias vulnerabilidades en el software de los dispositivos AMI que pueden ser explotadas por atacantes para tomar control de los sistemas. Estas vulnerabilidades incluyen fallos en la autenticación, errores de configuración y la falta de actualizaciones de seguridad.

En cuanto a las estrategias de mitigación, el uso de cifrado avanzado para la transmisión de datos se destacó como una de las más efectivas. Esto incluye el cifrado de extremo a extremo y el

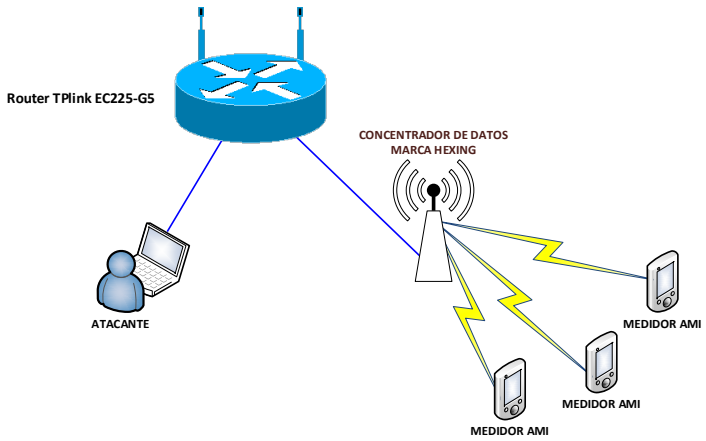
uso de protocolos seguros como TLS (Transport Layer Security). Implementar mecanismos de autenticación robustos, como la autenticación multifactor y el uso de certificados digitales, ayuda a garantizar que solo los usuarios y dispositivos autorizados puedan acceder a la red AMI.

La implementación de sistemas de monitoreo continuo y detección de intrusiones también resultó fundamental. Estos sistemas permiten identificar y responder rápidamente a actividades sospechosas en la red, incluyendo el uso de sistemas de detección de intrusiones basados en firmas y anomalías. Fortalecer la seguridad física de los dispositivos AMI mediante la instalación de sellos de seguridad, carcasas resistentes a manipulaciones y el uso de sensores que detecten intentos de intrusión física también es una medida crucial.

Las propuestas de mejora incluyeron la actualización regular del software de los dispositivos AMI. Mantener estos dispositivos actualizados con los últimos parches de seguridad y actualizaciones de software es esencial para proteger la red contra vulnerabilidades conocidas. Además, capacitar a los operadores y usuarios sobre las mejores prácticas de seguridad y concienciar sobre las amenazas potenciales puede mejorar significativamente la seguridad de las redes AMI. Desarrollar e implementar políticas de seguridad claras y estrictas, que incluyan la gestión de contraseñas, el control de acceso y la respuesta a incidentes, es crucial para mantener la integridad de la red.

Para la red AMI se realizó un monitoreo del flujo de paquetes, empleando Wireshark como herramienta principal de análisis. La Figura 1 muestra el diagrama de red utilizado en el escenario de prueba, donde se evidencian los diferentes dispositivos involucrados, incluyendo los medidores AMI, el concentrador de datos Hexing, el router TPLink EC225-G5 y un dispositivo atacante simulado. A través de este análisis, se logró identificar la dirección IP del concentrador de datos (192.168.0.101), que se confirmó como la puerta de enlace para la comunicación dentro de la red. La figura 1 muestra el diagrama red de la red AMI del caso de estudio.

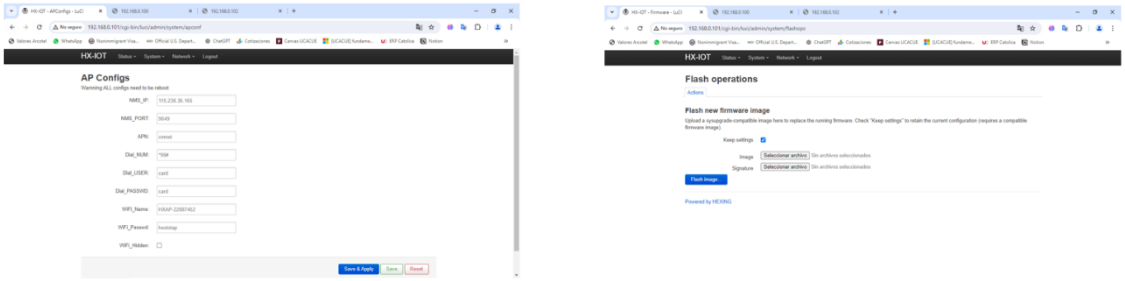
Figura 1. Diagrama de red de la red AMI.



Fuente: producción propia.

Basados en el análisis de los artículos de estudio, se obtuvo como resultado que los desafíos a los cuales se enfrenta el Serveless Computing están enfocados en: un correcto aislamiento de recursos, monitoreo de seguridad, gestión de seguridad y protección de datos, limitación de recursos para los usuarios, ampliación de la superficie de ataque, disponibilidad de los servicios, que las funciones de la nube se coloquen en la instancia de la VM, exposición de la interfaz, medidas de privacidad inadecuadas en microservicios y funciones, reducir la latencia de inicio, agotamiento de recursos financieros, y en el manejo de modelos de programación óptimos. La figura 2 muestra el acceso al dispositivo y configuraciones de firmware.

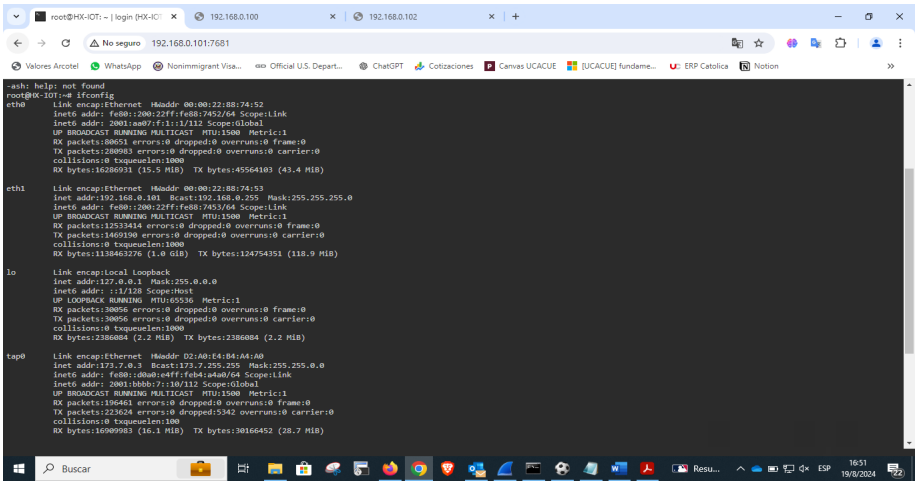
Figura 2. Configuraciones de firmware y autenticación



Fuente: producción propia.

Durante las pruebas, se detectó que el puerto 22 de SSH estaba expuesto, lo que permitió el acceso remoto al servicio del concentrador de datos mediante este protocolo. La Figura 3 representa el proceso de acceso al servicio SSH del concentrador, evidenciando una vulnerabilidad crítica que podría ser explotada por un atacante con conocimientos técnicos para obtener control sobre el dispositivo. La figura 3 muestra las configuraciones de acceso al servicio SSH.

Figura 3. Acceso al servicio SSH del concentrador

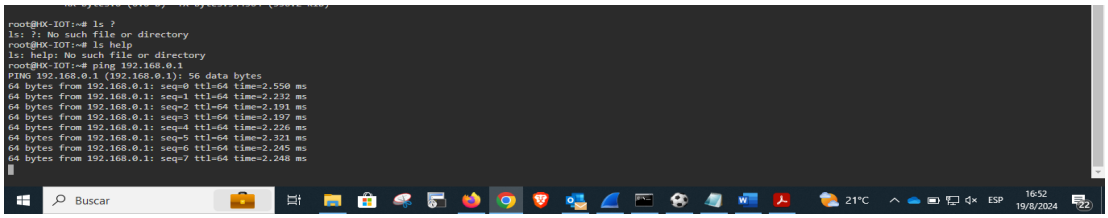


Fuente: producción propia.

Además, se realizaron pruebas de conectividad, incluyendo comandos de ping, desde el concentrador de datos hacia el router TPLink EC225-G5, validando la permanencia de la

comunicación entre estos equipos (Figura 4). Este experimento confirmó que, a pesar de las vulnerabilidades detectadas, la comunicación entre los dispositivos se mantenía estable, lo que resalta la importancia de implementar medidas de seguridad adicionales para proteger la integridad de la red. La figura 4 muestra las pruebas de conectividad desde el concentrador de datos hacia el router.

Figura 4. Pruebas de conectividad.



Fuente: producción propia.

Con base en los hallazgos obtenidos, y como discusión de los mismos, es recomendable el uso de contraseñas complejas y seguras en el concentrador de datos Hexing, integrando caracteres especiales, números, y letras mayúsculas y minúsculas.

Además, es necesario implementar listas de control de acceso en el router TPLink para restringir la conexión únicamente a usuarios autorizados. También, se debe limitar el acceso al concentrador de datos exclusivamente a través de SSH, bloqueando la interfaz web para minimizar el riesgo de explotación.

Un proceso seguro sería el de crear VLANs para separar los diferentes servicios y dispositivos dentro de la red, mejorando el control y la seguridad, y, finalmente, configurar el router para que se integre con un firewall, permitiendo un control más riguroso sobre el acceso al concentrador de datos

Conclusión

La seguridad en las redes de Medición Avanzada de Infraestructura (AMI) se presenta como un aspecto crítico y multifacético, demandando atención urgente y constante para garantizar la integridad, confiabilidad y resiliencia de las redes eléctricas inteligentes. La integración de tecnologías avanzadas en la infraestructura eléctrica tradicional ha introducido nuevos vectores de ataque y vulnerabilidades que deben ser abordados proactivamente.

Las redes AMI representan un componente esencial de las redes eléctricas inteligentes, permitiendo la recolección automática de datos de consumo energético y la gestión eficiente de los recursos. Sin embargo, estas redes son vulnerables a una variedad de amenazas de seguridad, incluyendo ataques de intercepción y manipulación de datos, intrusiones físicas, ataques de denegación de servicio (DoS) y explotación de vulnerabilidades en el software. La protección de estas redes es fundamental para asegurar la continuidad del suministro eléctrico, la exactitud en la facturación y la confianza del consumidor.

El estudio ha identificado múltiples amenazas significativas que pueden comprometer la seguridad de las redes AMI. La transmisión de datos sin cifrar expone la información a interceptaciones y manipulaciones, mientras que los dispositivos AMI son susceptibles a manipulaciones físicas que permiten el acceso no autorizado. Los ataques DoS pueden interrumpir la comunicación y operación de las redes, y las vulnerabilidades en el software pueden ser explotadas para tomar control de los sistemas. Estos riesgos subrayan la necesidad de implementar medidas de seguridad robustas y adaptativas.

Las estrategias de mitigación revisadas en este estudio incluyen el uso de cifrado avanzado para proteger la transmisión de datos, la implementación de mecanismos de autenticación fuerte, el monitoreo continuo de la red para detectar y responder a intrusiones, y la adopción de medidas físicas de seguridad para proteger los dispositivos AMI. Estas estrategias son efectivas para reducir los riesgos, pero deben ser complementadas con prácticas de actualización regular del software y una gestión de seguridad integral.

Para fortalecer la seguridad de las redes AMI, se proponen varias mejoras clave. La actualización regular del software es esencial para proteger contra vulnerabilidades conocidas. Además, la educación y capacitación de los operadores y usuarios sobre las mejores prácticas de seguridad y las amenazas potenciales pueden mejorar significativamente la seguridad. La implementación de políticas de seguridad claras y estrictas, que incluyan la gestión de contraseñas, el control de acceso y la respuesta a incidentes, es crucial para mantener la integridad de la red.

Este artículo destaca la necesidad de una investigación continua y multidisciplinaria para abordar las amenazas emergentes y desarrollar nuevas soluciones de seguridad. Las futuras líneas de investigación podrían enfocarse en el desarrollo de tecnologías de cifrado más avanzadas, la mejora de los sistemas de detección de intrusiones basados en inteligencia artificial y la creación de protocolos de seguridad específicos para los dispositivos AMI. Además, es importante explorar el impacto de las nuevas tecnologías, como el Internet de las Cosas (IoT) y el 5G, en la seguridad de las redes AMI.

Finalmente, la seguridad en las redes AMI es una preocupación crítica que debe ser abordada con urgencia y de manera integral. Las amenazas identificadas y las estrategias de mitigación discutidas en este estudio proporcionan una base sólida para mejorar la seguridad de estas redes. Sin embargo, es fundamental continuar desarrollando soluciones innovadoras y adaptativas para enfrentar las amenazas emergentes y garantizar la operación segura y fiable de las redes eléctricas inteligentes. La colaboración entre investigadores, industria y reguladores será clave para lograr estos objetivos y proteger la infraestructura crítica que sustenta nuestras sociedades modernas).

Referencias

Al-Soud, M. S., & Hrayshat, E. S. (2004). Rural photovoltaic electrification program in Jordan. *Renewable and Sustainable Energy Reviews, 8*(6), 593-598.

Arciniegas, M., Andrés, F., Imbajoa, R., David, E., & Revelo, F. J. (2017). Diseño e implementación de un sistema de medición inteligente para AMI de la microrred de la Universidad de Nariño. *Enfoque UTE, 8*(1), 300-314.

Chen, L., & Wang, Q. (2017). Cybersecurity for advanced metering infrastructure: A survey. *IEEE Transactions on Industrial Informatics, 13*(5), 2510-2519.

Davis, R., & Moore, S. (2018). Multifactor authentication: A critical review and future research agenda. *Journal of Information Security and Applications*, 42, 53-62.

Ehrler, V., & Hebes, P. (2012). Electromobility for city logistics–The solution to urban transport collapse? An analysis beyond theory. *Procedia–Social and Behavioral Sciences,* 48, 786-795.

Garcia, A., & Lee, J. (2018). Network segmentation in cybersecurity: A review of best practices and a case study in energy sector. *Journal of Cybersecurity, 3*(2), 155-167.

Hernandez, M., & Lopez, D. (2019). Defense in depth strategies against DoS attacks in smart grid communication networks. *International Journal of Electrical Power & Energy Systems,* 110, 319-327.

Kim, Y., & Park, S. (2020). Secure firmware validation for advanced metering infrastructure devices. *IEEE Transactions on Smart Grid, 11*(4), 3129-3139.

Meneses Ruiz, J. (2016). Aplicación de tecnologías de medición avanzada (AMI) como instrumento para reducción de pérdidas. *Boletín IIE.*

National Institute of Standards and Technology. (2010). *Guidelines for smart grid cyber security.*

Nguyen, H., & Kumar, P. (2018). Firmware security vulnerabilities in smart grid devices: Challenges and solutions. *Computers & Security,* 74, 184-197.

Autores

Jason Roberto Bermeo Varela. Ingeniero de Sistemas, 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.

Manuel Salvador Álvarez Vera. 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.