Vol.8 No.3 (2024): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.3.2024.2803-2816

Systematic review on 5G network security assessment methods

Revisión sistemática sobre los métodos de evaluación de la seguridad en redes 5G

Autores:

Astudillo-Villavicencio, Oscar Paúl
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la maestría en Ciberseguridad
Cuenca – Ecuador

oscar.astudillo.91@est.ucacue.edu.ec

https://orcid.org/0009-0009-4061-8781

Andrade-López, Miguel Santiago
UNIVERSIDAD CATÓLICA DE CUENCA
Docente tutor de la maestría en Ciberseguridad
Cuenca– Ecuador

msandradel@ucacue.edu.ec

https://orcid.org/0000-0002-6882-4204

Ureta-Arreaga, Laura Alexandra
UNIVERSIDAD CATÓLICA DE CUENCA
Docente de la maestría en Ciberseguridad
Cuenca– Ecuador

laura.ureta@ucacue.edu.ec

https://orcid.org/0000-0001-5328-8085

Fechas de recepción: 30-JUN-2024 aceptación: 06-AGO-2024 publicación:15-SEP-2024

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Este artículo revisa sistemáticamente los métodos tradicionales de evaluación de la seguridad en redes 5G, comparando su aplicabilidad y eficacia específica para abordar las vulnerabilidades inherentes a estas redes en constante evolución. Con la expansión continua de la tecnología 5G, emergen nuevas amenazas y desafíos de seguridad que requieren un análisis detallado y la adaptación de metodologías de seguridad tradicionales. Los métodos habituales, como las pruebas de penetración, análisis de riesgos y auditorías de seguridad, son evaluados capa por capa para identificar diversos tipos de vulnerabilidades que demandan técnicas específicas de evaluación y mitigación. Por ejemplo, la capa de enlace de datos se centra en amenazas relacionadas con la autenticación y autorización, mientras que la capa de red aborda problemas como la intercepción de datos y los ataques de denegación de servicio. Aunque estos métodos proporcionan una base sólida, su efectividad varía según la complejidad y especificidad de las redes 5G. Es crucial adaptar y mejorar estas técnicas para contrarrestar de manera efectiva las amenazas emergentes. Se destacan enfoques contemporáneos, como el uso de inteligencia artificial y aprendizaje automático para mejorar la detección y respuesta a amenazas en tiempo real.

Palabras clave: Redes 5G; Seguridad; Evaluación; Vulnerabilidades; Metodologías

Abstract

This article systematically reviews traditional methods for evaluating security in 5G networks, comparing their specific applicability and effectiveness in addressing inherent vulnerabilities in these constantly evolving networks. With the ongoing expansion of 5G technology, new threats and security challenges emerge, necessitating detailed analysis and adaptation of traditional security methodologies. Traditional methods such as penetration testing, risk analysis, and security audits are evaluated layer by layer to identify various types of vulnerabilities that require specific assessment and mitigation techniques. For instance, the data link layer focuses on threats related to authentication and authorization, while the network layer addresses issues such as data interception and denial-of-service attacks. Although these methods provide a solid foundation, their effectiveness varies depending on the complexity and specificity of 5G networks. Adapting and enhancing these techniques is crucial to effectively counter emerging threats. Contemporary approaches, such as the use of artificial intelligence and machine learning, are highlighted for improving real-time threat detection and response.

Keywords: 5G Networks; Security; Assessment; Vulnerabilities; Methodologies

Introducción

En la era de la conectividad inalámbrica, la implementación de redes 5G emerge como un hito tecnológico con el potencial de revolucionar las interacciones digitales. Sin embargo, esta evolución hacia la quinta generación de redes móviles también plantea desafíos cruciales en cuanto a seguridad cibernética.

La promesa de velocidades ultrarrápidas y una latencia mínima se ve acompañada por preocupaciones cada vez mayores sobre la vulnerabilidad de estas redes a diversas amenazas, desde ataques cibernéticos hasta la privacidad de los datos (Guerrero et al., 2023). A medida que las redes 5G se distribuyen a escala, existe cierto grado de invisibilidad ante amenazas inminentes. Proteger una red 5G requiere lidiar con ataques tradicionales, nuevos ataques y ataques que pueden surgir en el futuro (Salahdine et al., 2023)

El presente estudio se centra en afrontar el reto fundamental de explorar la revisión sistemática de los métodos de evaluación de seguridad en redes 5G, abordando las serias preocupaciones sobre vulnerabilidades debido a la arquitectura utilizada, cifrado frágil, autenticación débil o inseguridad en dispositivos finales (Poot Poot, 2022). Para contextualizar adecuadamente esta revisión sistemática, es esencial considerar los avances previos en el campo. Estudios anteriores han investigado aspectos específicos de la seguridad en redes 5G, desde el análisis de vulnerabilidades hasta la evaluación de protocolos de seguridad. Sin embargo, aún existe una brecha significativa en la comprensión de los métodos de evaluación utilizados para garantizar la seguridad en este contexto.

Los objetivos de este estudio son claros y definidos: primero, identificar los métodos existentes de evaluación de seguridad en redes 5G; segundo, evaluar críticamente la eficacia, aplicabilidad y limitaciones de estos métodos en el contexto de las demandas y desafíos únicos de las redes 5G; y tercero, comparar distintos enfoques de evaluación de la seguridad, destacando las mejores prácticas. La importancia de este estudio radica en su capacidad para abordar una necesidad urgente en el campo de la seguridad cibernética. Dada la creciente dependencia de las redes 5G en una variedad de sectores (desde la industria hasta la atención médica), comprender cómo evaluar y mitigar los riesgos de seguridad se vuelve crucial para garantizar la confiabilidad y la resiliencia de estas redes.

Los resultados de este estudio tienen el potencial de ser significativos. Al proporcionar una evaluación exhaustiva de los métodos de evaluación de seguridad en redes 5G, se puede informar y orientar la formulación de políticas en el campo de la ciberseguridad. Este artículo se encuentra organizado de la siguiente manera: en primer lugar, se presenta una introducción acerca de esta revisión; luego, se describe la metodología utilizada; a continuación, se lleva a cabo un análisis crítico a partir de las preguntas de investigación; y finalmente, se tienen las conclusiones y referencias de esta investigación.

Material y métodos

Se desarrolló una revisión sistemática en fuentes de información relevantes sobre los métodos de evaluación de la seguridad en redes 5G, considerando tres fases: 1) planificación de la investigación, 2) desarrollo de la búsqueda de literatura, y 3) información de resultados. La presente investigación se basó en los principios de los autores Kitchenham y Charters (2007), quienes proponen las directrices necesarias para desarrollar revisiones sistemáticas de literatura en la ingeniería de software.

Estas directrices tienen como objetivo guiar a los investigadores para que interpreten y evalúen las publicaciones disponibles mediante una pregunta de investigación específica. Este estudio abordó estas directrices para establecer una estructura clara en la elaboración de una revisión sistemática de literatura (RSL).

Primero, en la fase de planificación de la investigación, se formularon las siguientes preguntas: P1: ¿Cuántos estudios hacen referencia a la seguridad en redes 5G?, y P2: ¿Cómo se comparan los métodos tradicionales de evaluación de la seguridad, analizando su aplicabilidad y eficacia específica para abordar las vulnerabilidades presentes en las redes 5G? Para este estudio, se aplicaron reglas de inclusión y exclusión con el fin de determinar qué estudios serían considerados en la revisión. Estos incluyeron revisiones sistemáticas, revisiones de literatura, informes técnicos, normas y estándares de seguridad, y artículos relacionados con las preguntas de investigación planteadas. La revisión se realizó en el período comprendido entre los años 2021 y 2024.

A continuación, en la fase de desarrollo de la búsqueda de literatura, se llevó a cabo el proceso investigativo mediante la búsqueda en diversas fuentes de datos relacionadas con la literatura sobre métodos de evaluación de la seguridad en redes 5G. Se hizo uso de inteligencia artificial para facilitar esta búsqueda, resultando en la selección de un total de 55 documentos elegidos, tal como se muestra en la Tabla 1. Estos documentos fueron seleccionados en función de su relevancia y calidad, asegurando que proporcionaran una base sólida para la revisión sistemática.

Luego, la información de resultados se organizó y presentó de manera coherente y sistemática. Se analizaron los datos obtenidos de los documentos seleccionados, enfocándose en responder las preguntas de investigación y evaluar la eficacia de los métodos de evaluación de seguridad en redes 5G. Los resultados de este análisis proporcionan una visión integral de las prácticas actuales y destacan las áreas que requieren mayor atención y desarrollo en el futuro, como se observa en la Tabla 1.

Tabla 1

Resultados obtenidos de la búsqueda

Fuente	Palabras clave	Estudios relevantes	Documentos elegidos
Scopus		32	13
Ieee Xplore	Evaluation	40	18
Web of Science	Methods,	24	7
Science Direct	Security, 5G	18	5
Otros		12	12
TOTAL		**126**	**55**

Se llevó a cabo la revisión en fuentes como Scopus, IEEE Xplore, Web of Science, Science Direct y otros, obteniendo un total de 126 estudios relevantes colocando las palabras clave Evaluation Methods, Security, 5G. Posteriormente, se realizó una depuración de estudios que no cumplieron con los criterios establecidos mediante el resumen del documento encontrado, así como aquellos que se encontraron duplicados en diversas fuentes de información, eliminando un total de 71 trabajos de investigación, quedando 55 documentos elegidos, mismos que fueron fundamentales con la revisión de los métodos de evaluación de la seguridad en redes 5G.

Resultados

De acuerdo a lo indicado en la Tabla 1, se tiene un total de 55 documentos elegidos, de los cuales 32 artículos están relacionados específicamente con la seguridad en redes 5G. Estos artículos permiten entender la estructura multifacética de una red 5G, identificando componentes clave para la seguridad en estas redes. A continuación, se detalla la estructura de seguridad en redes 5G.

La seguridad en la red de acceso radio (RAN) abarca varios aspectos críticos. En cuanto a la autenticación, el 5G-AKA proporciona la autenticación mutua entre la red y el dispositivo del usuario (You et al., 2024). Asimismo, el EAP-AKA se utiliza para integrar la red 5G en la autenticación de redes no 3GPP, como WiFi (Zhang et al., n.d.). En términos de cifrado de datos y protección de integridad, se emplean algoritmos de cifrado como el 128-NEA (NEA1, NEA2, NEA3) dependiendo del nivel de seguridad requerido, mientras que los algoritmos de integridad más comunes son el NIA1, NIA2, y NIA3 (Poot Poot, 2022).

El aislamiento de red y slicing implica la implementación de ‘slices’ de redes virtuales con políticas de gestión y requisitos de seguridad específicos (Dhanasekaran et al., 2023). En la

seguridad del núcleo de la red (5GC), la protección de las interfaces internas del núcleo, como N1, N2, N3, y N4, se realiza mediante cifrado y autenticación (Khan & Chowdhury, 2021). La interconexión segura (SEPP) es esencial en escenarios de roaming, ofreciendo protección de integridad y cifrado de extremo a extremo en redes 5G.

La gestión de claves y el cifrado de datos en reposo son fundamentales para prevenir accesos no autorizados a los datos almacenados en el núcleo de la red. La distribución y gestión segura de las claves de cifrado (KMS) y el cifrado de datos en reposo son prácticas estándar. El control de acceso y las políticas de seguridad se implementan mediante NFV y SDN, aplicando políticas de seguridad adaptativas, creando virtualización dentro de la red y redes definidas por software. Además, el AMF y SMF gestionan sesiones y acceso, implementando controles de políticas de seguridad, autenticación y autorización (Bolívar Rolando Quizhpe Vásquez et al., 2023).

El monitoreo y la respuesta a incidentes también se benefician del uso de NFV y SDN, que aplican políticas de seguridad adaptativas dentro de la red. La integración de la seguridad RAN y 5GC se gestiona de manera coordinada, garantizando una transición segura mediante protocolos de seguridad que protegen la comunicación entre el núcleo de la red y la RAN.

En cuanto a la conformidad y regulación, la utilización y cumplimiento de estándares como 3GPP TS 33.501, TSI TR 103 305, y NIST SP 800-187 aseguran que se sigan las mejores prácticas para la seguridad en redes 5G (Salvador & Rajnai, 2023). La tecnología 5G presenta un progreso notable en el área de las comunicaciones móviles, pero su rápida expansión y la introducción de infraestructuras virtualizadas requieren un estudio detallado de las implicaciones de seguridad y sus aplicaciones en sistemas de información.

Garantizar una adecuada gestión de la seguridad de la información es vital para prevenir riesgos que podrían afectar los desarrollos basados en 5G. El despliegue de esta tecnología presenta diversos desafíos y riesgos de seguridad que deben abordarse de manera integral, ya que la mayor capacidad de conectividad y la densidad de dispositivos aumentan la superficie de ataque, especialmente con la incorporación masiva de dispositivos IoT.

La importancia crítica de 5G en infraestructuras esenciales como redes eléctricas y sistemas de transporte implica que cualquier ataque o vulnerabilidad podría tener consecuencias graves. Además, las nuevas tecnologías introducidas, como NFV y la segmentación de red, ofrecen beneficios, pero también presentan desafíos de seguridad que deben ser abordados.

La dependencia del software y las interfaces abiertas incrementa el riesgo de vulnerabilidades y ataques, haciendo esencial la protección de la privacidad de los datos debido a la cantidad y sensibilidad de la información transmitida (Fernández Fernández et al., 2024). Los proveedores de servicios y fabricantes de componentes desarrollan constantemente tecnologías y actualizan las especificaciones de seguridad con el fin de mitigar nuevas vulnerabilidades en las redes inalámbricas (DHS & Odni, 2021).

Para realizar la comparación de los métodos tradicionales de evaluación de la seguridad en redes 5G, es necesario indicar que se va a analizar capa por capa de acuerdo al modelo OSI, como se observa en la tabla 2, presentando vulnerabilidades, amenazas y posibles soluciones

Tabla 2

Capas del modelo OSI (De acuerdo a la Organización Internacional para la Normalización ISO)

CAPAS DEL MODELO OSI	
Número de Capa	**Nombre de Capa**
7	Capa de Aplicación
6	Capa de Presentación
5	Capa de Sesión
4	Capa de Transporte
3	Capa de Red
2	Capa de Enlace de datos
1	Capa física

Capa de Aplicación | Capa 7

En la capa de Aplicación del modelo OSI, crucial para la interacción usuario-servicio, se destacan métodos tradicionales como pruebas de aplicaciones web y móviles, y análisis estático y dinámico de código. Estos métodos enfrentan desafíos significativos en entornos 5G debido a la integración con servicios en la nube y dispositivos IoT, lo cual requiere enfoques específicos para abordar vulnerabilidades únicas.

Por ejemplo, aplicaciones como redes vehiculares, blockchain, redes basadas en la información, redes definidas por software y sistemas de inteligencia artificial presentan amenazas como transmisiones no cifradas, ataques DDoS, y vulnerabilidades en APIs y modelos de aprendizaje, respectivamente. Las soluciones incluyen cifrado de extremo a extremo, algoritmos de consenso robustos, mejoras en controladores SDN, mecanismos de autenticación para APIs, y técnicas de entrenamiento adversarial para modelos de IA.

Capa de Presentación | Capa 6

En la capa de Presentación, la compresión y el cifrado de datos continúan siendo cruciales para la eficiencia y seguridad de la transmisión de datos en redes 5G. Sin embargo, deben ser rápidos para no afectar el rendimiento crítico en tiempo real de estas redes, dada la alta movilidad y concurrencia de dispositivos. Las vulnerabilidades incluyen inserción de datos maliciosos, desbordamiento de buffer en aplicaciones y vulnerabilidades asociadas a la criptografía. Las soluciones propuestas incluyen inteligencia artificial para monitoreo de tráfico, seguridad basada en la nube con firewalls y sistemas de prevención de pérdida de

datos (DLP), y protocolos de cifrado robustos como TLS 1.3 con cifrado de extremo a extremo.

Capa de Sesión | Capa 5

En la capa de Sesión, la gestión segura de sesiones es fundamental para mantener la integridad de las comunicaciones en entornos 5G, aunque la alta movilidad de dispositivos representa un desafío para su implementación efectiva. Las amenazas como el secuestro y falsificación de sesiones requieren técnicas avanzadas de automatización para mantener la seguridad. Las soluciones incluyen autenticación multifactor (MFA), políticas de tiempo de espera adecuadas y la adopción del modelo Zero Trust.

Capa de Transporte | Capa 4

En la capa de Transporte, el cifrado TLS/SSL sigue siendo esencial para proteger los datos en tránsito en redes 5G, aunque enfrenta desafíos como la latencia ultra baja y la alta velocidad. Las vulnerabilidades incluyen ataques de intermediarios, DoS/DDoS, inyección de paquetes y explotación de vulnerabilidades en protocolos como TCP/UDP. Las soluciones propuestas incluyen la optimización del cifrado TLS/SSL, firewalls de próxima generación (NGFW), filtrado y validación de paquetes, y sistemas de detección de intrusiones (IDS).

Capa de Red | Capa 3

En la capa de Red, los sistemas IPS/IDS y firewalls son esenciales para proteger la infraestructura de red en entornos 5G, aunque deben adaptarse a la virtualización de funciones de red (NFV) y la naturaleza distribuida de estas redes. Las vulnerabilidades incluyen ataques de enrutamiento, DoS/DDoS y explotación de protocolos de red como BGP y OSPF. Las soluciones incluyen protocolos de enrutamiento seguro, segmentación de red, y actualizaciones frecuentes de seguridad.

Capa de Enlace de Datos | Capa 2

En la capa de Enlace de Datos, la detección de anomalías y el control de acceso son fundamentales para asegurar la autenticación de dispositivos en redes 5G, especialmente con la proliferación de dispositivos IoT. Las vulnerabilidades como el spoofing de MAC y ARP requieren soluciones como protocolos de seguridad PSCP y RLC, Dynamic ARP Inspection (DAI), y políticas QoS para gestionar el tráfico.

Capa Física | Capa 1

En la capa Física, la protección contra interferencias y accesos no autorizados es crucial, especialmente con la densidad de nodos y el uso de frecuencias altas en redes 5G. Las vulnerabilidades incluyen interferencia de señales y ataques de relé y replay. Las soluciones propuestas incluyen técnicas como el espectro ensanchado por salto de frecuencia (FHSS), y el uso de cifrado robusto para garantizar la confidencialidad de las señales.

Discusión

Los resultados de esta revisión sistemática destacan avances significativos en los métodos de evaluación de la seguridad en redes 5G a lo largo de los años, particularmente en detección de amenazas, gestión de vulnerabilidades y protección de datos. Estos avances reflejan una respuesta proactiva hacia la complejidad creciente y las demandas de seguridad de las redes 5G. Sin embargo, es importante señalar que existen desafíos substanciales que aún requieren atención.

La constante evolución de las tecnologías 5G implica que algunos de los métodos más recientes y prometedores no hayan sido incluidos en nuestra revisión debido a la limitación del periodo de búsqueda. Esta limitación temporal subraya la necesidad de investigaciones continuas y actualizadas para capturar las últimas innovaciones en seguridad cibernética aplicadas a redes 5G.

Además, la diversidad de metodologías de evaluación encontradas en los estudios revisados dificulta una comparación directa de resultados. Esta variabilidad puede atribuirse a las diferentes interpretaciones de los estándares de seguridad, así como a las estrategias específicas adoptadas por cada estudio para abordar las amenazas emergentes en las redes 5G.

Para futuras investigaciones, se recomienda enfocarse en la integración de tecnologías emergentes como Inteligencia Artificial y Blockchain. Estas tecnologías tienen el potencial de fortalecer aún más la seguridad en redes 5G mediante métodos avanzados de detección y respuesta automatizada ante amenazas. Asimismo, es crucial establecer estándares y regulaciones que aseguren una protección homogénea y efectiva en todos los niveles de implementación de redes 5G.

Además, se enfatiza la importancia de adoptar una evaluación continua de la seguridad, implementando enfoques flexibles que permitan adaptarse rápidamente a nuevas amenazas y vulnerabilidades. Este enfoque adaptativo es fundamental para garantizar la robustez y confiabilidad a largo plazo de las infraestructuras de redes 5G en un entorno digital dinámico y en constante evolución.

Conclusiones

La seguridad en las redes 5G requiere una evolución continua de los métodos tradicionales de evaluación y la adopción de técnicas específicas. La adaptabilidad, la integración de medidas proactivas y la capacitación constante son esenciales para garantizar la integridad, confidencialidad y disponibilidad de estas redes.

Aunque los métodos tradicionales de evaluación de seguridad, como el análisis de vulnerabilidades, las pruebas de penetración y las auditorías de seguridad, siguen siendo relevantes, necesitan una evolución significativa para abordar las particularidades de las

tecnologías 5G. Esto incluye la virtualización de funciones de red (NFV) y las redes definidas por software (SDN). La capacidad de adaptarse a las nuevas arquitecturas y dinámicas de las redes 5G es crucial para mantener una evaluación de seguridad eficaz y actualizada.

Un enfoque proactivo y multifacético es fundamental para mitigar las vulnerabilidades y responder a las amenazas en las redes 5G. Esto implica implementar y evaluar técnicas robustas de cifrado, segmentación de red, políticas de control de acceso y sistemas avanzados de monitorización y detección de anomalías. Además, la capacitación y concienciación constante del personal en prácticas de seguridad y gestión de incidentes son vitales. La capacidad de responder rápidamente a las amenazas emergentes y mantener una evaluación continua de las medidas de seguridad garantiza la protección de esta infraestructura crítica y en constante evolución.

La seguridad en las redes 5G no solo depende de herramientas y técnicas avanzadas, sino también de la capacidad de adaptación y respuesta ante un panorama de amenazas dinámico. La evolución continua de los métodos de evaluación, junto con una vigilancia activa y una cultura organizacional centrada en la seguridad, son fundamentales para asegurar la robustez y fiabilidad de las redes 5G en el futuro digital.

Referencias bibliográficas

Abdi, A. H., Audah, L., Salh, A., Alhartomi, M. A., Rasheed, H., Ahmed, S., & Tahir, A. (2024). Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3393548

Alsmadi, I., Aljaafari, N., Nazzal, M., Alhamed, S., Sawalmeh, A. H., Vizcarra, C. P., Khreishah, A., Anan, M., Algosaibi, A., Al-Naeem, M. A., Aldalbahi, A., & Al-Humam, A. (2022). Adversarial Machine Learning in Text Processing: A Literature Survey. *IEEE Access*, *10*, 17043–17077. https://doi.org/10.1109/ACCESS.2022.3146405

Bolívar Rolando Quizhpe Vásquez, I., Juan Gabriel Ochoa Aldeán, I., & Sc, M. (2023). *Análisis de la seguridad en redes 5G y propuesta de mejoras*. https://dspace.unl.edu.ec//handle/123456789/27469

Desai, B. V., Kamath, Y. G., Rao, D. P., Anusha, S., & Belgaonkar, S. M. (2022). Implementation of Physical Layer Encryption for Wireless Communication System. *2022 IEEE North Karnataka Subsection Flagship International Conference, NKCon 2022*. https://doi.org/10.1109/NKCON56289.2022.10126923

Dhanasekaran, R. M., Ping, J., & Gomez, G. P. (2023). End-to-End Network Slicing Security Across Standards Organizations. *IEEE Communications Standards Magazine*, *7*(1), 40–47. https://doi.org/10.1109/MCOMSTD.0005.2200055

DHS, & Odni. (n.d.). *SECURITY IMPLICATIONS OF 5G TECHNOLOGY: Overview and Recommendations*.

Estado del arte de la infraestructura de la tecnología 5G enfocada a la capa física. (2022). Barrera, María. https://repository.usta.edu.co/handle/11634/42900

Fernández Fernández, F. J., Fernández Gavilanes, M. (advisor), & Fondo Ferreiro, P. (advisor). (2024). *La tecnología 5G, amenazas para la seguridad y oportunidades para los sistemas de información*. Centro Universitario de la Defensa en la Escuela Naval Militar. http://calderon.cud.uvigo.es/handle/123456789/759

Guerrero, B., Oswaldo, M., & Moya, G. (2023). Ciberseguridad en las redes 5G: desafíos y soluciones. *Revista Científica y Tecnológica VICTEC*, *4*(7), 63–73. https://doi.org/10.61395/VICTEC.V4I7.114

Jagan, S., Pokhariyal, R., Mahajan, K., Deepika, C. L. N., Sudha, P. D., & Dutta, A. (2023). Machine Learning with Deep Learning Approach for Cyber Security Threats Prevention Model. *Proceedings of the 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2023*. https://doi.org/10.1109/ICSES60034.2023.10465570

Khan, J. A., & Chowdhury, M. M. (2021). Security Analysis of 5G Network. *IEEE International Conference on Electro Information Technology*, *2021-May*, 1–6. https://doi.org/10.1109/EIT51626.2021.9491923

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering

Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M., & Martinelli, F. (2021). Privacy for 5G-Supported Vehicular Networks. *IEEE Open Journal of the Communications Society*, *2*, 1935–1956. https://doi.org/10.1109/OJCOMS.2021.3103445

Miao, Y., Yan, X., Li, X., Xu, S., Liu, X., Li, H., & Deng, R. H. (2024). RFed: Robustness-Enhanced Privacy-Preserving Federated Learning Against Poisoning Attack. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.2024.3402113

Muzammil, M. Bin, Bilal, M., Ajmal, S., Shongwe, S. C., & Ghadi, Y. Y. (2024). Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking. *IEEE Access*, *12*, 6365–6375. https://doi.org/10.1109/ACCESS.2024.3350444

Omar, T., Griffin, B., & Garcia, J. (2023). ML based Detection and Mitigation Scheme for DoS attacks on SDN Controllers. *Proceedings - 2023 IEEE Conference on Dependable and Secure Computing, DSC 2023*. https://doi.org/10.1109/DSC61021.2023.10354117

Poot Poot, J. E. (2022). Seguridad en redes 5G. *Exploraciones, Intercambios y Relaciones Entre El Diseño y La Tecnología*, 57–79. https://doi.org/10.16/CSS/JQUERY.DATATABLES.MIN.CSS

Salahdine, F., Han, T., & Zhang, N. (2023). Security in 5G and beyond recent advances and future challenges. *Security and Privacy*, *6*(1), e271. https://doi.org/10.1002/SPY2.271

Salvador, L. R., & Rajnai, Z. (2023). 5G Standardization Process: An Overview. *SISY 2023 - IEEE 21st International Symposium on Intelligent Systems and Informatics, Proceedings*, 571–574. https://doi.org/10.1109/SISY60376.2023.10417964

Seçgin, S. (2023). Seven Layers of ISO/OSI. *Evolution of Wireless Communication Ecosystems*, 41–50. https://doi.org/10.1002/9781394182343.CH5

Shah, M. S. M., Leau, Y. B., Anbar, M., & Bin-Salem, A. A. (2023). Security and Integrity Attacks in Named Data Networking: A Survey. *IEEE Access*, *11*, 7984–8004. https://doi.org/10.1109/ACCESS.2023.3238732

Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A Survey of IoT and Blockchain Integration: Security Perspective. *IEEE Access*, *9*, 156114–156150. https://doi.org/10.1109/ACCESS.2021.3129697

Sullivan, S., Brighente, A., Kumar, S. A. P., & Conti, M. (2021). 5G Security Challenges and Solutions: A Review by OSI Layers. *IEEE Access*, *9*, 116294–116314. https://doi.org/10.1109/ACCESS.2021.3105396

Xie, M., Liu, J., Chen, S., & Lin, M. (2023). A survey on blockchain consensus mechanism: research overview, current advances and future directions. *International Journal of Intelligent Computing and Cybernetics*, *16*(2), 314–340. https://doi.org/10.1108/IJICC-05-2022-0126/FULL/XML

You, I., Kim, G., Shin, S., Kwon, H., Kim, J., & Baek, J. (2024). 5G-AKA-FS: A 5G Authentication and Key Agreement Protocol for Forward Secrecy. *Sensors (Basel, Switzerland)*, *24*(1). https://doi.org/10.3390/S24010159

Zhang, J., Yang, L., Cao, W., & Wang, Q. (n.d.). *Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif*. https://doi.org/10.1109/ACCESS.2020.2969474

Zhong, H., Wang, L., Cui, J., Zhang, J., & Bolodurina, I. (2023). Secure Edge Computing-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks. IEEE Transactions on Information Forensics and Security, 18, 3774–3786. https://doi.org/10.1109/TIFS.2023.3287731

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.