La integración de la biometría en el internet de las cosas: desafíos y oportunidades

The Integration Of Biometry In The Internet Of Things: Challenges And Opportunities

Melvin Kevin López Asto, Alberto Carlos Mendoza de los Santos

Universidad Nacional de Trujillo, Trujillo, Perú

Resumen

En este documento se presenta un análisis exhaustivo basdo en una revisión sistemática que sigue las directrices del enfoque PRISMA. El análisis aborda las complejidades y posibilidades relacionadas con la integración de la biometría en el Internet de las Cosas (IoT) durante el periodo de 2018 a 2023, centrándose específicamente en aspectos de seguridad, eficiencia y aplicaciones prácticas. Utilizando como base de datos PubMed, Scopus y DOAJ, se inició con un total de 125 artículos. Sin embargo, tras aplicar criterios estrictos de selección, solo 18 de estos fueron considerados aptos para la revisión. La biometría, que alude a la determinación y confirmación sobre la identificación de un individuo centrándose en atributos corporales o comportamentales únicas, se postula como una herramienta crucial para fortalecer la seguridad en creciente ámbito del IoT. Esta combinación promete mayor confiabilidad en la autenticación, pero también plantea inquietudes sobre privacidad. Las ventajas incluyen la autenticación trifactorial, protección avanzada de información médica, mayor seguridad en transacciones financieras móviles y autenticaciones basadas en múltiples rasgos biométricos. Estas integraciones biotecnológicas potencian la seguridad de los dispositivos IoT, dificultando ataques y suplantaciones, garantizando la autenticidad y protección de la información de los usuarios.

Palabras Claves: Biometría, IoT, Internet de las Cosas, Autenticación, Seguridad

Abstract

This paper presents a comprehensive analysis based on a systematic review following the guidelines of the PRISMA approach. The analysis addresses the complexities and possibilities related to the integration of biometrics in the Internet of Things (IoT) during the period from 2018 to 2023, focusing specifically on aspects of security, efficiency, and practical applications. Using PubMed, Scopus and DOAJ as databases, it started with a total of 125 articles. However, after applying strict selection criteria, only 18 of these were considered suitable for review. Biometrics, which alludes to the determination and confirmation of an individual's identification by focusing on unique bodily or behavioral attributes, is posited as a crucial tool for strengthening security in the growing IoT arena. This combination promises greater reliability in authentication, but also raises privacy concerns. Advantages include three-factor authentication, advanced protection of medical information, increased security in mobile financial transactions, and authentications based on multiple biometric traits. These biotech integrations enhance the security of IoT devices, making attacks and spoofing more difficult, ensuring the authenticity and protection of user information.

Keywords: Biometrics, IoT, Internet of Things, Authentication, Security

INTRODUCCIÓN

La intersección entre la biometría y el Internet de las Cosas (IoT) ha emergido como un campo de estudio crucial en la actualidad. Este documento tiene la intención de exponer los hallazgos de una revisión sistemática completa, utilizando el enfoque metodológico PRISMA, que abarca la investigación realizada durante los últimos seis años en este intrigante campo de estudio. La biometría, que se basa en medidas físicas y comportamentales exclusivas de una persona, ofrece un método fiable para verificar la identidad. En paralelo, el IoT permite la recopilación y análisis de datos en diversos campos, incluida la autenticación biométrica a través de sensores de movimiento y biométricos.

La relación entre la biometría y el IoT se vuelve esencial para garantizar la seguridad y autenticación en dispositivos y sistemas conectados. La biometría añade una capa adicional de protección al IoT al permitir la identificación a través de características únicas como huellas dactilares o reconocimiento facial, garantizando así que únicamente individuos autorizados puedan acceder a la información y los dispositivos relacionados con el IoT. Esta integración resulta de vital importancia para preservar la privacidad y la legitimidad de los datos en un contexto donde la interconexión es ubicua y la seguridad se erige como una preocupación de máxima importancia.

Además, en este documento se explora a profundidad la sinergia entre la biometría y el IoT, resaltando sus beneficios, desafíos y aplicaciones. A lo largo de este informe, se examinará cómo la incorporación de la biometría en el IoT mejora la seguridad y la autenticación en dispositivos conectados.

MATERIALES Y MÉTODOS

La revisión sistemática que se presenta aquí se realizó siguiendo las directrices establecidas por el enfoque PRISMA (Elementos de Reporte Preferidos para Revisiones Sistemáticas y Meta-Análisis). La cuestión de estudio que orientó este estudio se formuló de la siguiente manera: ¿Cuáles son los principales desafíos y oportunidades vinculados a la incorporación de la biometría en el Internet de las Cosas (IoT) durante los últimos seis años en lo que respecta a seguridad, eficacia y usos prácticos?

Rossi (2023) y Khan, Bueno-Cavanillas y Zamora (2022) coinciden en que una revisión sistemática es un método metódico y exhaustivo para recopilar y sintetizar la información actual

relacionada con una pregunta de investigación. Según ambas fuentes, su objetivo principal es producir un resumen objetivo y completo de la evidencia disponible en dicho contexto, lo que permite decidir con base en la evidencia más sólida y contribuye al avance del conocimiento en un campo específico. Básicamente, ambas descripciones resaltan la significancia de ser minucioso y completo al identificar, seleccionar y evaluar estudios pertinentes con el fin de ofrecer resultados que sean válidos, exactos y beneficiosos en relación con una pregunta de investigación concreta.

PubMed, Scopus y DOAJ fueron las bases de datos principales utilizadas para iniciar la búsqueda de artículos en inglés. Se aplicó un filtro para que solo se consideraran las publicaciones de los últimos seis años, es decir, de 2018 a 2023.

La primera búsqueda avanzada en PubMed se llevó a cabo utilizando los términos siguientes:

- (integration of biometrics OR biometrics in IoT) AND (challenges OR difficulties) AND opportunities AND (2018:2023[pdat])

Del mismo modo, se ejecutó una exploración detallada en el repositorio de datos Scopus siguiendo los siguientes parámetros:

- (integration AND of AND biometrics OR biometrics AND in AND iot) AND (challenges OR difficulties) AND opportunities
  Además, se debe que tener presente, que se limito el año de publicación ente 2018 y 2023. El tipo de documento debe ser "Article". El área temática deber ser "Engineering" y "Computer Science". Finalmente, como palabras clave se tuvieron en cuenta los siguientes términos "Internet of Things", "Authentication" y "Biometrics".

Por último, se efectuaron exploraciones en la sección de artículos de la base de datos DOAJ utilizando los términos "Biometrics", "Internet of Things" y "Authentication" a la vez esos términos se utilizaron como palabras clave, limitando la asignatura a "Technology" y restringiendo los años de publicación desde 2028 hasta 2023.

En resumen, se encontraron 19 resultados en la búsqueda avanzada de PubMed, 101 resultados en Scopus y 5 resultados en DOAJ. Antes de comenzar el análisis de los artículos, se fijaron criterios para decidir cuáles serían incorporados y cuáles serían excluidos.

Criterio de inclusión:

- Artículos sobre la biometría en el Internet de las cosas.
- Artículos sobre la seguridad, la eficiencia y las aplicaciones prácticas de esta integración.
- Artículos divulgados en el período más reciente de 6 años (de 2018 a 2023).

Criterio de exclusión:

Los artículos que no cumplían con el formato de un artículo académico y los que se enfocaban en áreas que no eran relevantes para una revisión sistemática fueron excluidos.

Se llevó a cabo una selección minuciosa de los artículos siguiendo estrictamente los criterios establecidos. En una primera etapa, después de una evaluación inicial basada en sus títulos, se eliminaron un total de 88 artículos. Luego se leyó el resumen de los artículos restantes. Aquí, se descartaron otros 17 artículos porque no presentaban la información necesaria sobre la integración de la biometría en el Internet de las cosas (IoT). Además, se excluyeron dos documentos por su inaccesibilidad en la nube o por falta de acceso completo a ellos.

Tras un riguroso proceso de selección, solamente 18 artículos lograron satisfacer plenamente los requisitos de inclusión. La Figura 1 presenta una selección de 10 de estos artículos, los cuales desempeñan un papel fundamental en nuestra investigación en curso. Es esencial destacar que estos documentos se centran en la integración de la biometría en el contexto del IoT y, lo que es aún más relevante, muchos de ellos demuestran la aplicación práctica de la

biometría en dicho entorno.

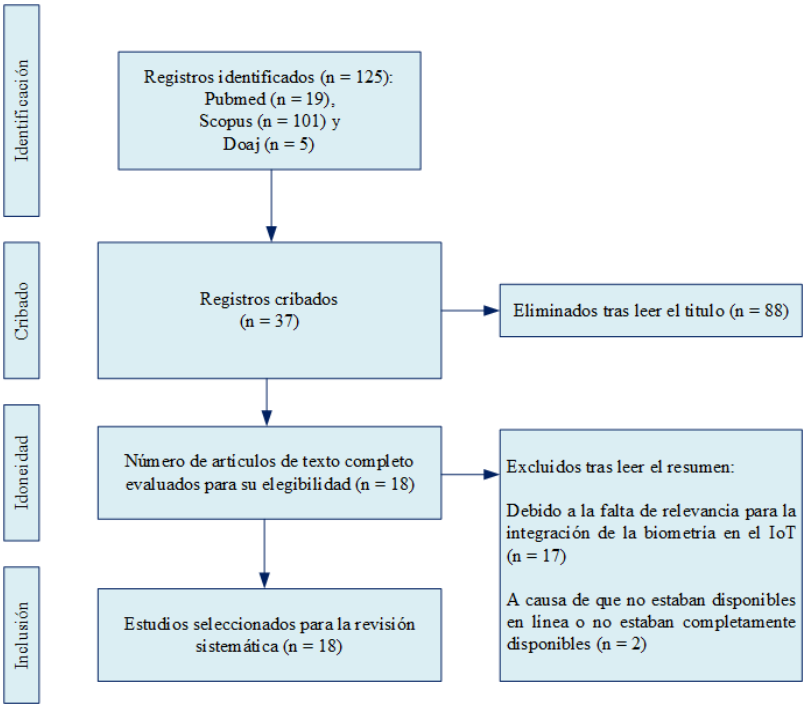

Figura 1. Representación gráfica de la Metodología PRISMA en cuatro niveles.

RESULTADOS Y DISCUSIÓN

A continuación, se presenta la Tabla 1, que resume algunos de los artículos más relevantes.

N°	Autor	Artículo	País	Año	Principales desafíos y oportunidades relacionados con la integración de la biometría en el Internet de las Cosas
1	Pourbemany Jafar, Zhu Ye, Bettati Riccardo	A Survey of Wearable Devices Pairing Based on Biometric Signals	Estados Unidos	2023	Lo más sobresaliente de este artículo es la posibilidad de aprovechar señales biométricas y contextos compartidos para incrementar la protección y la eficiencia en la comunicación entre dispositivos wearables. Al mismo tiempo, señala desafíos relacionados con la seguridad, la diversidad de sensores y la privacidad que deben abordarse en futuras investigaciones y desarrollos en este campo.
2	Batool Samera, Hassan Ali, Khattak Muazzam A. Khan, Shahzad Ahsan, Farooq Muhammad Umar	IoTAuth: IoT Sensor Data Analytics for User Authentication Using Discriminative Feature Analysis	Pakistan	2022	El artículo destaca la oportunidad de utilizar sensores biomédicos y análisis de datos en entornos de IoT para abordar los desafíos de seguridad y privacidad en la autenticación de usuarios. Estos enfoques presentan una notable precisión y eficinecia e el proceso de autenticación, o cual puede resultar vetajoso en una amplia gama de aplicaciones relacionadas con el IoT, tales como la atención médica digital y el desarrollo de ciudades inteligentes.
3	Deebak B. D., Al-Turjman Fadi, Aloqaily Moayad, Alfandi	An Authentic-Based Privacy Preservation Protocol for Smart	Estados Unidos	2019	La implementación de la autenticación basada en biometría en las aplicaciones de atención médica basadas en IoT ofrecen una oportunidad para abordar los desafíos

	Omar	e-Healthcare Systems in IoT			relacionados con la seguridad, privacidad y eficiencia de recursos. Además, hay pruebas que respaldan la eficacia de la propuesta para salvaguardar la información médica confidencial y mejorar la eficiencia de los recursos en los sistemas electrónicos inteligentes de asistencia sanitaria.
4	Shin Sooyeon, Taekyoung Kwon	A Lightweight Three-Factor Authentication and Key Agreement Scheme in Wireless Sensor Networks for Smart Homes	Corea del Sur	2019	Aborda desafíos de seguridad y eficiencia en hogares inteligentes basados en redes de sensores inalámbricos (WSN). Propone un esquema de autenticación de tres factores que incorpora tarjetas inteligentes, contraseñas y biometría para fortalecer la seguridad. Esto ofrece oportunidades para sistemas de hogar inteligente más seguros y eficientes, con posibilidades de investigaciones prácticas futuras para evaluar su efectividad en el mundo real.
5	Eman Raihan Dewon, Jahan Mosarrat, Kabir Upama	A multi-device user authentication mechanism for Internet of Things	Reino Unido	2023	Propone un esquema de autenticación basado en contraseñas de un solo uso (OTP) que permite a los usuarios acceder desde múltiples dispositivos en un entorno IoT, mejorando la usabilidad. El artículo destaca la importancia de la autenticación en la seguridad de la red IoT y demuestra la viabilidad y eficiencia de su enfoque a través de análisis de lógica BAN, herramientas AVISPA y evaluaciones de rendimiento.
6	Khan Saad, Parkinson Simon, Grant Liam, Liu Na, Mcguire Stephen	Biometric Systems Utilising Health Data from Wearable Devices: Applications and Future Challenges in Computer Security	Estados Unidos	2020	Se centra en el contexto de la salud y el monitoreo médico. En otras palabras, enfatiza que los datos de salud generados por dispositivos portátiles IoT ofrecen valiosas oportunidades en seguridad informática, especialmente en sistemas biométricos para identificación y autenticación.
7	Torre Damiano, Chennamaneni Anitha, Rodriguez Alex	Privacy-Preservation Techniques for IoT Devices: A Systematic Mapping Study	Estados Unidos	2023	Destaca la importancia de abordar la privacidad en IoT y presenta hallazgos de un estudio que identificó 260 investigaciones sobre técnicas de preservación de la privacidad en dispositivos IoT. La mayoría se enfoca en el uso de técnicas criptográficas para mejorar la autenticación, pero la falta de compartición de implementaciones sugiere la necesidad de colaboración.
8	Ali Guma, Dida Mussa Ally, Elikana Sam Anael	A secure and efficient multi-factor authentication algorithm for mobile money applications	Tanzania	2021	Aborda la seguridad en las aplicaciones de dinero móvil en países en desarrollo y presenta un nuevo algoritmo de autenticación multifactor. Dado que las aplicaciones de dinero móvil a menudo dependen solo de la autenticación de dos factores, como PIN y tarjeta SIM, son vulnerables a ataques. El algoritmo propuesto combina PIN, contraseña de un solo uso y huella dactilar biométrica para mejorar la seguridad. Los prototipos de aplicaciones móviles desarrollados muestran que este enfoque es eficaz y

					puede beneficiar a usuarios, proveedores de servicios y gobiernos al garantizar transacciones seguras de dinero móvil.
9	Farid Farnaz, Elkhodr Mahmoud, Sabrina Fariza, Ahamed Farhad, Gide Ergun	A smart biometric identity management framework for personalized IoT and cloud computing-based healthcare services	Australia	2021	Destaca la relevancia de la biometría en la protección y confidencialidad de los sistemas de atención médica personalizados basados en IoT y la nube. Propone un marco donde se utiliza rasgos biométricos encriptados multimodales para la autenticación, combinando señales de electrocardiograma (ECG) y fotopletismograma (PPG). La inclusión de la encriptación homomórfica garantiza que los datos de los pacientes permanezcan seguros incluso cuando se procesan en la nube, lo que cierra la puerta a muchos ataques de seguridad tradicionales.
10	Ahmed Yaser Fahad Alsahlani, Alexandru Popa	LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment	Rumanía	2021	En respuesta al desafió de COVID-19, se presenta LMAAS-IoT, un esquema de autenticación multifactorial para IoT en entornos basados en la nube. Utilizando técnicas criptográficas y un extractor difuso para información biométrica, garantiza la seguridad y eficiencia de los datos en tiempo real. Tal propuesta destaca por su robustez y practicidad, marcando un avance significativo en la protección de sistemas IoT.

Tabla 1. Aspectos destacados de los artículos seleccionados.

Fundamentos de la biometría en el IoT

1. **Biometría:**
   Se trata de la exploración y evaluación de las medidas físicas y comportamentales únicas de un individuo, que se utilizan para identificar y verificar su identidad de manera confiable. La autenticación biométrica implica la comparación de los datos biométricos obtenidos de una persona con su plantilla biométrica para determinar la semejanza. Dado que los datos biométricos están intrínsecamente vinculados a los rasgos y características distintivas de un individuo, es poco probable que dos individuos compartan datos biométricos idénticos. Esto mejora la confiabilidad de autenticación biométrica como método de seguridad física (Annadurai et al, 2022; Khan H. U. et al, 2023; Yang et al, 2023).
2. **Internet de las cosas (IoT):**
   Se refiere a una tecnología ubicua que permite la interconexión de diversos dispositivos y sensores a través de Internet para recopilar, transmitir y analizar datos, abarcando aplicaciones en campos como la teledetección, ciudades inteligentes y atención médica digital remota. Además, el IoT implica la generación masiva de datos con posibles aplicaciones, incluyendo la autenticación biométrica de usuarios mediante sensores de movimiento y biométricos (Torre et al, 2023; Batool et al, 2022).
3. **Relación entre la biometría y el IoT:**
   La relación entre la biometría y el IoT es fundamental en la autenticación y seguridad de dispositivos y sistemas conectados. La biometría proporciona una capa adicional de seguridad al IoT al permitir la identificación y verificación de usuarios a través de rasgos únicos, como huellas dactilares o reconocimiento facial. Esto resulta crucial para asegurar que únicamente individuos con autorización puedan acceder a los dispositivos o información del IoT, salvaguardando, de esta manera, la confidencialidad y la

consistencia de la información en un entorno donde la conectividad es constante y la seguridad se vuelve de máxima importancia.

Según Pourbemany et al. (2023), la interacción entre la biometría e IoT es evidenciado principalmente en el ámbito de los dispositivos wearables, donde se aprovechan las señales biométricas, como el movimiento del cuerpo o el ritmo cardíaco, para crear protocolos de emparejamiento seguro. Asimismo, cabe resaltar que, aunque esto promete seguridad y conveniencia, también plantea preocupaciones urgentes sobre la privacidad y autonomía. Por otro lado, en Eman et al. (2023), se propone un esquema de autenticación basado en OTP para usuarios de IoT desde múltiples dispositivos. La OTP se genera independientemente por ambas partes, garantizando seguridad sin compartir la contraseña. Este método atiende la necesidad de autenticación segura y adaptable en el creciente universo IoT. Destaca la importancia de evolucionar en las prácticas de autenticación, en el campo del IoT. La idea de generar OTPs de forma independiente es un reflejo ingenioso de cómo la tecnología puede reconfigurarse para ofrecer soluciones más seguras, al mismo tiempo que se adapta a la multifacética naturaleza de acceso de los usuarios en la actualidad.

Ventajas de la integración de la biometría en el IoT

Aquí tienes una tabla que resume las ventajas de la integración de la biometría en el IoT y cómo mejora la seguridad y autenticación.

Ventajas	Cómo mejora la seguridad y la autenticación en los dispositivos IoT
Según Shin y Kwon (2019), autenticación trifactorial.	Al combinar la biometría con tarjetas inteligentes y contraseñas, se proporciona a un mayor nivel de seguridad, lo que dificulta la suplantación de identidad y mejora la resiliencia contra posibles ataques.
Según Deebak et al. (2019), protección mejorada de la información sensible del paciente.	La implementación del esquema SAB-UAS (Secure and Anonymous Biometric Based User Authentication Scheme) garantiza una autenticación de usuario basada en biometría que es segura y anónima, evitando que adversarios accedan a la información. Esto asegura que solo los profesionales médicos autorizados puedan acceder a los datos, y establece comunicaciones seguras entre dispositivos a través de una clave de sesión secreta.
Según Ali et al. (2021), mejora significativa en la seguridad de las transacciones de dinero móvil.	Al hacer uso de la huella dactilar como uno de los factores en un sistema de autenticación multifactorial, se refuerza la seguridad al ser difícil de réplica o falsificar, proporcionando una robustez contra ataques como suplantación, MITM (Man-In-The-Middle), etc.
Según Farid et al. (2021), autenticación rápida, fiable y segura.	Al utilizar una combinación de electrocardiograma (ECG) y señales de fotopletismograma (PPG) para la autenticación. Tal fusión, provoca una autenticación más robusta y segura, cerrado la puerta a muchos ataques de seguridad tradicionales, entre ellos suplantación (spoofing). Asimismo, el uso de encriptación homomórfica (HE) permite que los daos de los pacientes permanezcan cifrados incluso cuando se procesas o analizan en la nube. En otras palabras, garantiza autenticación segura basada en rasgos biológicos únicos y que la información del paciente se mantenga segura y privada.
Según Alsahlani y Popa (2021), autenticación ligera y multifactorial.	Al incorporar detalles biométricos del usuario con la ayuda del Fuzzy Extractor, se establece una identificación singular que minimiza riesgos de suplantación. Paralelamente, técnicas criptográficas avanzadas, como funciones hash unidireccionales junto con operaciones XOR, actúan como escudos adicionales contra intrusiones. Esta arquitectura, junto con un protocolo de reconocimiento bilateral entre usuario y dispositivo, y rigurosas validaciones de seguridad, optimiza la resiliencia del sistema.

Tabla 2. Ventajas principales de la integración de la biometría en la autenticación IoT.

Desafíos de seguridad en la integración

Teniendo como punto de partida la Tabla 2, es claro que la biometría en el IoT presenta notables ventajas en seguridad y autenticación. No obstante, también se debe reconocer que

con estas ventajas emergen desafíos particulares. Paradójicamente, muchas de las fortalezas que la biometría introduce en el IoT son, al mismo tiempo, puntos de atención que deben ser gestionados para asegurar su efectividad total. Como resultado, la siguiente tabla se deriva directamente del contenido de la Tabla 2.

Desafío de seguridad en la biometría	Amenaza	Posible solución
Autenticación trifactorial	Suplantación de identidad	Combinar biometría con tarjetas inteligentes y contraseñas
Protección de información sensible	Intrusos accediendo a la información.	Hacer uso del esquema SAB-UAS
Seguridad en transacciones móviles	Ataques MITM, suplantación	Uso de huella dactilar en sistema de autenticación multifactorial
Autenticación rápida y segura	Suplantación, ataques tradicionales	Fusionar ECG con PPG y usar HE
Autenticación ligera y multifactorial	Riesgos de suplantación	Detalles biométricos con Fuzzy Extractor, funciones hash unidireccionales, operaciones XOR, y reconocimiento bilateral

Tabla 3. Desafíos de seguridad en biometría para IoT: Amenazas, análisis y soluciones.

Tecnologías biométricas en el IoT

Las tecnologías biométricas, junto con el IoT, se han consolidado como dos pilares fundamentales en el panorama tecnológico contemporáneo. Su unión representa una innovación crucial para asegurar una autenticación fiable y personalizada en dispositivos interconectados. La integración de estás tecnologías con el IoT, permite que dispositivos como cerraduras, wearables o vehículos autónomos verifiquen rápidamente la identidad del usuario de forma confiable, optimizando su experiencia y reduciendo el riesgo de accesos no autorizados.

Las tecnologías biométricas, dentro del contexto del Internet de las Cosas Médicas (IoMT) cabe especificar que es una rama del IoT, están revolucionando el monitoreo y la prevención de enfermedades. Estos dispositivos capturan, procesan y envían información biométrica, proponiendo soluciones innovadoras en el sector salud (Sim y Cho, 2023). Se presentarán algunos ejemplos en la Figura 2.

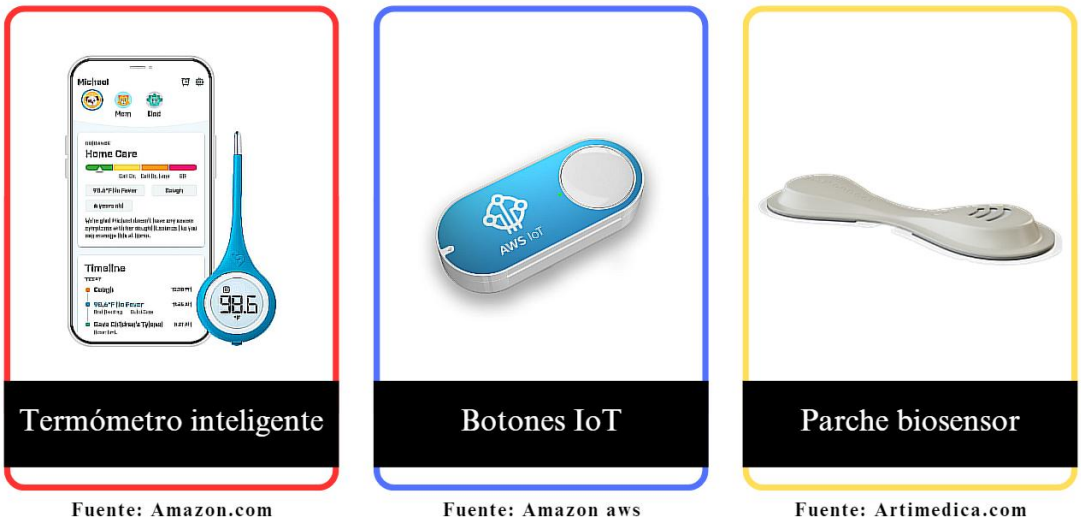

Figura 2. IoMT: Innovaciones biométricas en salud.

Según Sim y Cho (2023):

- **Termómetro inteligente:** Este dispositivo conectado a internet permite detectar y enviar información sobre fiebres altas.
- **Botones IoT:** Fueron diseñados para mantener altos estándares de higiene en hospitales

de Canadá, notifican de forma inmediata sobre infecciones hospitalarios para minimizar riesgos.

- **Parche biosensor:** Es un adhesivo liviano y de un solo uso que se ubica en el pecho del individuo y registra en tiempo real la temperatura, frecuencia cardíaca, ECG y patrón respiratorio.

Por otra parte, según Rukhiran et al. (2023), en el sector educativo, la incorporación de tecnologías biométricas, en particular para verificar la identidad de estudiantes durante exámenes, muestra resultados prometedores. A diferencia de los métodos tradicionales de monitoreo, los cuales pueden ser vulnerables a manipulaciones y desaciertos, los dispositivos biométricos IoT presentan una alternativa más segura, dinámica y rentable.

Según Chen et al. (2021), las herramientas tecnológicas biométricas IoT, permite que los dispositivos puedan adaptarse instantáneamente a las necesidades de los estudiantes por ende mejorar su experiencia de aprendizaje.

CONCLUSIONES

La incorporación de la tecnología biométrica en el IoT brinda perspectivas prometedoras para el fortalecimiento de la seguridad y la optimización de la eficiencia en diversos ámbitos, tales como wearables, atención médica y sistemas de hogares inteligentes. Sin embargo, estas oportunidades generan desafíos relacionados con la protección de datos personales y la variedad de dispositivos de detección.

La convergencia entre la biometría y el IoT, tal como se evidencia en los dispositivos wearables, presenta mejoras sustanciales en cuanto al nivel de seguridad que brindan. Sin embargo, persisten desafíos en relación a la privacidad y la autonomía del usuario. Los métodos de autenticación, como las OTPs autogeneradas, reflejan la necesidad por adaptarse y optimizar la seguridad en un entorno IoT en constante crecimiento.

La integración de tecnologías biométricas en el IoT ha transformado varios sectores, desde la seguridad y la salud hasta la educación. En el sector médico, el IoMT aprovecha dispositivos como termómetros inteligentes, botones IoT y parches biosensores para monitorear y prevenir enfermedades de manera innovadora. Además, en el dominio de la formación académica, las tecnologías biométricas del ámbito del IoT proporciona una vía segura y adaptable para autenticar la identidad de los estudiantes en exámenes, ajustándose a las particularidades individuales de cada estudiante con el objetivo de mejorar su experiencia de aprendizaje.

REFERENCIAS BIBLIOGRÁFICAS

Ali, G., Dida, M. A., & Elikana Sam, A. (2021). *A secure and efficient multi-factor authentication algorithm for mobile money applications*. Future Internet, 13(12), 299. https://doi.org/10.3390/fi13120299

Alsahlani, A. Y. F., & Popa, A. (2021). LMAAS-IoT: *Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment*. Journal of Network and Computer Applications, 192(103177), 103177. https://doi.org/10.1016/j.jnca.2021.103177

Annadurai, C., Nelson, I., Devi, K., Manikandan, R., Jhanjhi, N., Masud, M., & Sheikh, A. (2022). *Biometric authentication-based intrusion detection using artificial Intelligence Internet of Things in smart city*. Energies, 15(19), 7430. https://doi.org/10.3390/en15197430

Batool, S., Hassan, A., Khattak, M. A. K., Shahzad, A., & Farooq, M. U. (2022). *IoTAuth: IoT sensor data analytics for user authentication using discriminative feature analysis*. IEEE access: practical innovations, open solutions, 10, 59115–59124. https://doi.org/10.1109/access.2022.3178635

Chen, X., Zou, D., Xie, H., & Wang, F. L. (2021). *Past, present, and future of smart learning:*

a topic-based bibliometric analysis. International Journal of Educational Technology in Higher Education, 18(1). https://doi.org/10.1186/s41239-020-00239-6

Deebak, B. D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2019). *An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT*. IEEE access: practical innovations, open solutions, 7, 135632–135649. https://doi.org/10.1109/access.2019.2941575

Eman, R. D., Jahan, M., & Kabir, U. (2023). *A multi-device user authentication mechanism for Internet of Things*. IET Networks, 12(5), 229–249. https://doi.org/10.1049/ntw2.12088

Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). *A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services*. Sensors (Basel, Switzerland), 21(2), 552. https://doi.org/10.3390/s21020552

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). *Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis*. IEEE access: practical innovations, open solutions, 11, 80181–80198. https://doi.org/10.1109/access.2023.3298824

Khan, K. S.; Bueno-Cavanillas, A.; & Zamora, J. (2022). *Revisiones sistemáticas en cinco pasos: II. Cómo identificar los estudios relevantes*. Medicina de Familia. SEMERGEN, 48(6), 431-436. https://doi.org/10.1016/j.semerg.2021.12.006

Lien, C.-H., & Sudip Vhaduri. (2023). Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey. ACM Computing Surveys, 56(1), 1–37. https://doi.org/10.1145/3603705

Pourbemany, J., Zhu, Y., & Bettati, R. (2023). *A survey of wearable devices pairing based on biometric signals*. IEEE access: practical innovations, open solutions, 11, 26070–26085. https://doi.org/10.1109/access.2023.3254499

Rossi, E. (2023). *Introducción a las revisiones sistemáticas y metaanálisis*. Acta gastroenterologica Latinoamericana, 53(1), 7–14. https://doi.org/10.52787/agl.v53i1.291

Rukhiran, M., Wong-In, S., & Netinant, P. (2023). *IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach*. IEEE access: practical innovations, open solutions, 11, 22767–22787. https://doi.org/10.1109/access.2023.3253024

Torre, D., Chennamaneni, A., & Rodriguez, A. (2023). *Privacy-preservation techniques for IoT devices: A systematic mapping study*. IEEE access: practical innovations, open solutions, 11, 16323–16345. https://doi.org/10.1109/access.2023.3245524

Shin, S., & Kwon, T. (2019). *A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes*. Sensors (Basel, Switzerland), 19(9), 2012. https://doi.org/10.3390/s19092012

Sim, S., & Cho, M. (2023). *Convergence model of AI and IoT for virus disease control system*. Personal and Ubiquitous Computing, 27(3), 1209–1219. https://doi.org/10.1007/s00779-021-01577-6

Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). *A review of homomorphic encryption for privacy-preserving biometrics*. Sensors (Basel, Switzerland), 23(7), 3566. https://doi.org/10.3390/s23073566