INGENIERÍA INVESTIGA

Vol. 4, e711, año 2022
ISSN – Online: 2708-3039
DOI: https://doi.org/10.47796/ing.v4i0.711

Artículo de Revisión

BENEFICIOS DE LAS TECNOLOGÍAS BIOMÉTRICAS PARA LA AUTENTICACIÓN DE USUARIOS: UNA REVISIÓN SISTEMÁTICA

BENEFITS OF BIOMETRIC TECHNOLOGIES FOR USER AUTHENTICATION: A SYSTEMATIC REVIEW

VICTOR ENRIQUE LEON PAZ[1]
https://orcid.org/0000-0002-6058-551X

JHON ANTONY LIVIAS CERQUIN[2]
https://orcid.org/0000-0001-8975-3073

ALBERTO CARLOS MENDOZA DE LOS SANTOS[3]
https://orcid.org/0000-0002-0469-915X

Recibido: 29/11/2022
Aceptado: 23/12/2022
Publicado: 28/09/2022

[1, 2,3] Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, La Libertad, Perú

E-mail: [1]vleon@unitru.edu.pe, [2]jlivias@unitru.edu.pe, [3]amendozad@unitru.edu.pe

Facultad de Ingeniería
Publicación Oficial

Resumen

Con el avance tecnológico a menudo los sistemas guardan la información personal y confidencial de los usuarios sin autenticación o en algunos casos con autenticación limitada, por ejemplo, técnicas de autenticación externa basadas en el conocimiento con una contraseña convencional, en este contexto la tecnología biométrica encamina una nueva forma de autenticación para proteger la información por tal razón, el objetivo de esta investigación sistemática de literatura científica se enfoca en la importancia que tiene las tecnologías biométricas para la autenticación de usuarios, por consiguiente el estudio se realizó siguiendo la metodología PRISMA usando como fuente de información, las publicaciones de la base de datos SCOPUS de los últimos 5 años; se encontraron 5 688 artículos, seleccionando 23 artículos después de aplicar los filtros de exclusión e inclusión. El análisis Efectuado permite concluir que los beneficios más relevantes que aportan las tecnologías biométricas en la autenticación de usuarios es el aumento de la seguridad cuando se realiza el control de acceso, al igual que el ahorro de esfuerzo y tiempo al no tener que recordar una contraseña.

Palabras clave: Autenticación de usuario; biometría; tecnología biométrica.

Abstract

With technological advances, systems often store the users personal and confidential information without authentication or in some cases limited authentication, for instance, external authentication techniques based on knowledge with a conventional password, in this context, biometric technology leads to a new form of authentication to protect the information. For this reason, the objective of this systematic investigation of scientific literature focuses on the importance of biometric technologies for user authentication. Therefore, the study was carried out following the PRISMA methodology using the publications of the SCOPUS database from the last 5 years as a source of information; selecting 23 articles after applying exclusion and inclusion filters. The analysis led to the conclusion that the most relevant benefits of biometric technologies in user authentication are: increased security when access control is performed, as well as saving effort and time by not having to remember a password.

Keywords: User authentication; biometrics; biometric technology.

1. Introducción

La biometría y sus aplicaciones en el medio con respecto a la falsificación y robo de documentos de identidad, son respuestas frente a la ciberdelincuencia, y los cambios que están surgiendo frente a los avances tecnológicos. Una de las tecnologías referenciadas es la autenticación biométrica, la cual utiliza las características fisiológicas y del comportamiento para autenticar lo manifestado por el usuario. Además, se ha establecido rápidamente como el medio más pertinente para identificar y autenticar individuos de una manera rápida y confiable, a través del uso de las características biológicas únicas (Zhou & Ren, 2018).

En la actualidad, con el avance tecnológico, el empleo de términos como sistematizar, se está volviendo cada vez más popular con una gran variedad de servicios o procesos. Sin embargo, en el pasado, solo había dos maneras de comprobar la identidad del usuario, ya sea por medio de algún objeto físico que usted posea o por algo que guarde en la mente. Debido a que esto, siempre se consideró que era un tema relativamente simple de implementar, ya sea mediante el uso de objetos como una llave para el ingreso a la casa, los documentos de identidad, la placa de los autos o por palabras o frases que uno guarda en la mente, específicamente para el uso de contraseñas ya sea para acceder al email, a la cuenta de una red social, etc.

Debido a la necesidad de resguardar información sensible, se implementa la autenticación del usuario, tal como sostienen Usoltsev et al. (2022) al afirmar que por medio de una parte de su cuerpo, la huella digital, la mano, la cara, el cual estaba reservada para aplicaciones sensibles, como la seguridad de los sitios militares, sin embargo, ahora se está desarrollando rápidamente, a través de aplicaciones de dominio público.

En este sentido, Laka (2021) considera que muchos sistemas de autenticación pueden verse comprometidos hoy en día si se utilizan como una solución de autenticación de un solo factor motivo por el cual se requiere más de una técnica de autenticación elegida de independientes categorías de credenciales sugiriendo la implementación de métodos biométricos tanto en términos de comportamiento como fiscalidad. Además, considera el análisis del cuerpo humano como una nueva e identificadora inexplorada que se puede emplear para el usuario final autenticado.

La biometría se encarga de estudiar y analizar las características físicas o el comportamiento propio de cada ser humano, con el objetivo de demostrar la identidad de manera irrefutable, usando aquello que hace a uno diferente. En este sentido, se clasifican en dos categorías muy importantes que son las tecnologías biométricas-fisiológicas y del comportamiento (Gehrmann et al., 2019).

Las formas más comunes de la biometría son las del comportamiento como; la dinámica de la firma, el reconocimiento de voz, la dinámica de la pulsación de las teclas, la manera en que se utilizan los objetos, los gestos, la marcha, el sonido de los pasos, etc. Con respecto a las fisiológicas, hay diferentes formas de medir que consisten, principalmente, en el ojo (iris y retina), el patrón de las venas, la forma de la mano, del dedo, las huellas dactilares y la forma de la cara que son los objetivos principales de mucha investigación científica (Zhang et al., 2022).

Usualmente, se espera que las mediciones fisiológicas sean más precisas en el sujeto a examinar. Por ejemplo, no están tan sujetas a los efectos del estrés, en comparación con la

identificación mediante la medición del comportamiento (Jaswal, 2021).

La identificación biométrica consiste en determinar la identidad de una persona mediante la comparación de las características de la persona con las que ya se tiene guardadas. La función principal es obtener las características biométricas, por ejemplo, fotografiando el rostro, huella dactilar, grabar la voz, y lograr identificar si el rostro, la voz, o la huella dactilar de la persona coincide con los recopilados (Kausar, 2020).

Según la Real Academia Española (2014), se conoce como tecnología, el conjunto de instrumentos y procedimientos industriales de un determinado sector o producto; por lo que la tecnología biométrica permite automatizar y perfeccionar el proceso de la identificación biométrica, logrando que esta tecnología se aplique con varias finalidades, en especial con la seguridad.

Por lo tanto, la investigación tuvo el objetivo de responder a la pregunta ¿Qué beneficios tiene la tecnología biométrica en la autenticación de usuarios?

2. Métodos

La revisión sistemática de la literatura se realizó sobre la base del modelo PRISMA, el cual permite organizar y analizar todos los artículos con los se van a trabajar, para luego sintetizar las evidencias que ayudan a dar respuesta a la incógnita planteada. Este paso se da de forma objetiva y reproducible. La revisión sistemática efectuada es una recopilación de una serie de manuscritos encontrados en la base de datos SCOPUS, que permiten conocer de manera clara los beneficios de tener las tecnologías de biométricas para la autenticación de usuarios.

2.1. Proceso de recolección de información

Para ejecutar la búsqueda de los artículos, primero se identificaron los términos relacionados con el tema de investigación, tales como: biometría, autenticación de usuarios, Autenticación biométrica. Las palabras claves se tradujeron al idioma inglés, siendo en orden de prelación Biometrics, User authentication, Biometrics authentication, para la realización de la conexión lógica de los términos se utilizaron los términos booleanos *AND Y OR*.

2.2. Proceso de selección

Todos los artículos se recopilaron desde la base de datos SCOPUS y se empleó la cadena de búsqueda (ARTICLE TITLE, ABSTRACT, KEYWORDS [Biometrics] AND ARTICLE TITLE, ABSTRACT, KEYWORDS [User authentication]); al hacer la búsqueda con la cadena se obtuvieron un total de 5 688 resultados. Una vez obtenido ese resultado, se aplicó el filtro para obtener solo los documentos publicados desde el 2018 hacia adelante, con este filtro de exclusión quedaron 2 504 resultados de la búsqueda.

Posteriormente, se consideró excluir los documentos que no eran artículos, al llevar a cabo el filtrado disminuyo a 1096 artículos. A continuación, se aplicó la exclusión de los artículos que no tenían que ver con autenticación biométrica, quedando con 142 artículos para la revisión sistemática. Seguidamente, se realizó la exclusión de los artículos que no estaban relacionados con ciencias de la computación, Ingeniería y Matemáticas, quedando 97 artículos.

Finalmente, se excluyó los artículos a los que no se tenía acceso, quedando 23 artículos para efectuar la revisión sistemática. Los criterios de exclusión se muestran en la Tabla 1.

Tabla 1

Criterios de Exclusión

N.°	Criterios de Exclusión
CE1	Excluir las publicaciones anteriores al 2018
CE2	Excluir las publicaciones que no sean de artículos
CE3	Excluir los artículos que no tenga relación con "autenticación biométrica"
CE4	Excluir los artículos que no tenga relación con "Ingeniería" y "Matemáticas"
CE5	Excluir los artículos que no tienen acceso libre

Nota. CE = criterios de exclusión.

3. Resultados

Después recopilar los artículos científicos desde la base de datos SCOPUS, aplicando la cadena de búsqueda y aplicar los filtros antes señalados, se analizó los 23 artículos que contienen información relevante, tal como se observa en la tabla 2.

Tabla 2

Lista de artículos incluidos en la revisión sistemática

N.°	Título	Autores	Año
1	Voice Response Questionnaire System for Speaker Recognition Using Biometric Authentication Interface	- Kao, Chang Yi - Chueh, Hao En	2023
2	Mining Hidden Partitions of Voice Utterances using Fuzzy Clustering for Generalized Voice Spoofing Countermeasures	- Altuwayjiri, Sarah Mohammed - Bchir, Ouiem - Maher, Mohamed - Ismail, Ben.	2022
3	A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques	- Albalawi, Shoroog - Alshahrani, Lama - Albalawi, Nouf - Kilabi, Reem - Alhakamy, aeshah	2022
4	A novel multimodal hand database for biometric authentication	- Bharath, M. R. - Rao, K. A. Radhakrishna	2022
5	VOLERE: Leakage Resilient User Authentication Based on Personal Voice Challenges	- Zhang, Rui - Yan, Zheng; Wang, Xuerui - Deng, Robert	2022
6	- A Proposed Biometric Authentication Model to Improve Cloud Systems Security	- El-El-Sofany, Hosam	2022

Tabla 2 (continuación/1)

N.°	Título	Autores	Año
7	User Authentication Method via Speaker Recognition and Speech Synthesis Detection	- Park, Hyun - Kim, Taeguen	2022
8	Cancelable Speaker Identification System Based on Optical-Like Encryption Algorithms	- El-Gazar, Safaa - El-Shafai, Walid - El-Banby, Ghada - Hamed, Hesham F. A. - Salama, Gerges M. - Abd-Elnaby, Mohammed - El-Samie, Fathi E. Abd	2022
9	Adversarial Attacks Impact on the Neural Network Performance and Visual Perception of Data under Attack	- Usoltsev, Yakov - Lodonova, Balzhit - Shelupanov, Alexander - Konev, Anton - Kostyuchenko, Evgeny	2022
10	A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users	- Kovalan, Krishnapriyaa - Omar, Siti Zobidah - Tang, Lian - Bolong, Jusang - Abdullah, Rusli - Ghazali, Akmar Hayati Ahmad - Pitchan, Muhammad Adnan	2021
11	Dorsal hand vein authentication system using artificial neural network	- Chin, Sze Wei - Tay, Kim Gaik - Chew, Chang Choon - Huong, Audrey - Rahim, Ruzairi Abdul	2021
12	AI-Biometric-Driven Smartphone App for Strict Post-COVID Home Quarantine Management	- Jaswal, Gaurav - Bharadwaj, Rohit - Tiwari, Kamlesh - Thapar, Daksh - Goyal, Piyush - Nigam, Aditya	2021
13	Secure Online Examination with Biometric Authentication and Blockchain-Based Framework	- Zhu, Xiaoling - Cao, Chenglong	2021
14	Novel user authentication method based on body composition analysis	- Laka, Pawel - Korzeb, Zbigniew - Mazurczyk, Wojciech	2021
15	Password policy characteristics and keystroke biometric authentication	- Parkinson, Simon - Khan, Saad - Crampton, Andrew - Xu, Qing; Xie, Weizhi - Liu, Na - Dakin, Kyle	2021

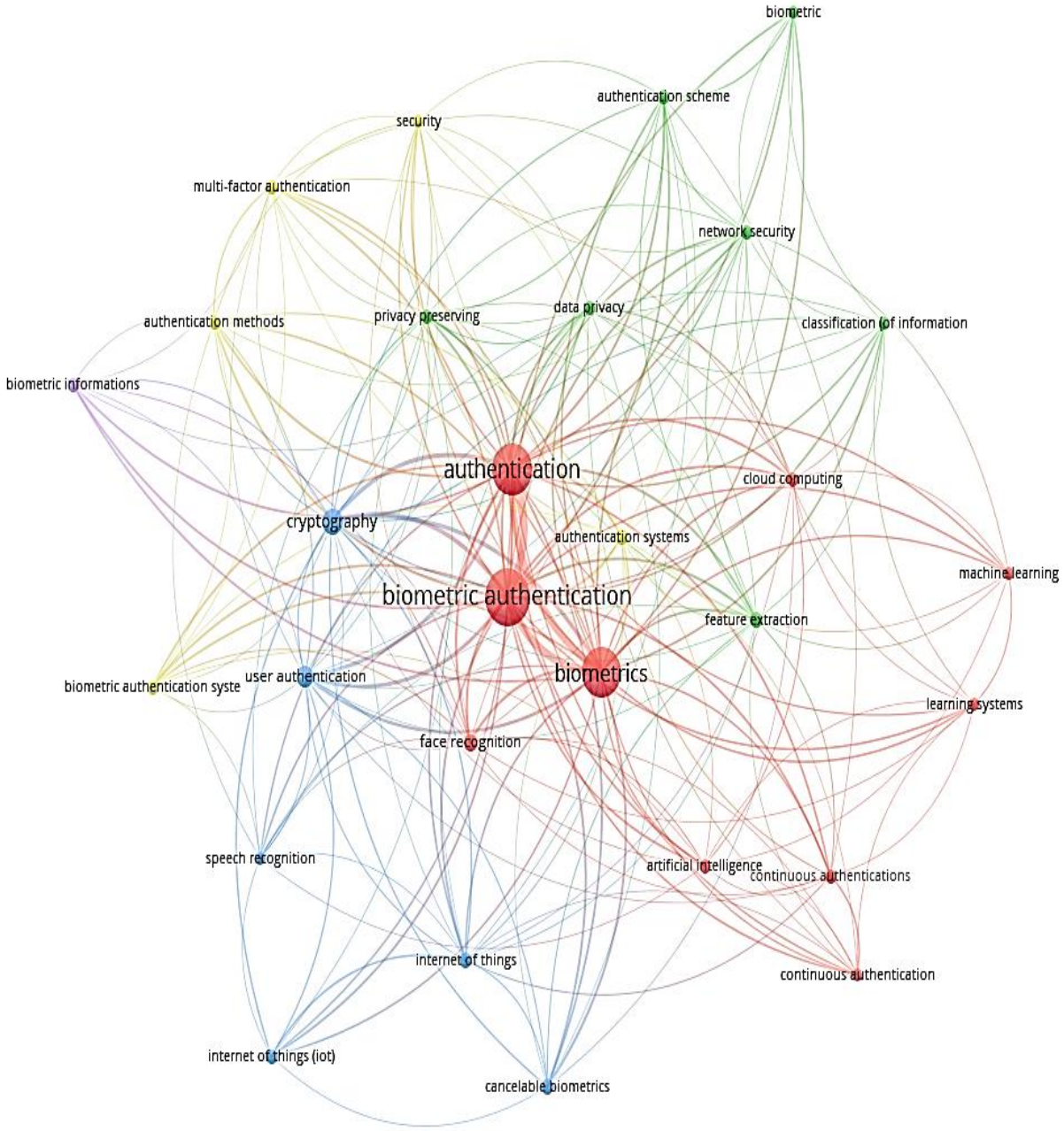
Tabla 2 (continuación/2)

N.°	Título	Autores	Año
16	Cancelable Face Template Protection using Transform Features for Cyberworld Security	- Kausar, Firdous	2020
17	Enhanced authentication system performance based on keystroke dynamics using classification algorithms	- Salem, Asma - Sharieh, Ahmad - Sleit, Azzam - Jabri, Riad.	2019
18	User behavioral analysis using Markov chain and steady-state in tracer and checker model	- Arun, V. - Sudhakar, R.	2019
19	A Cancelable Template for the Low-Quality Fingerprints from Wearable Devices	- Lee, Sanghoon - Jeong, Ik Rae - Araujo, Alvaro.	2019
20	Metadata filtering for user-friendly centralized biometric authentication	- Gehrmann, Christian - Rodan, Marcus - Jönsson, Niklas	2019
21	Comments on "PassBio: Privacy-preserving user-centric biometric authentication"	- Zhou, Kai - Ren, Jian	2018
22	Biometric authentication and verification for medical cyber physical systems	- Alhayajneh, Abdullah - Baccarini, Alessandro N. - Weiss, Gary M. - Hayajneh, Thaier - Farajidavar, Aydin.	2018
23	Multibiometric Fusion Authentication in Wireless Multimedia Environment Using Dynamic Bayesian Method	- Wu, Zhendong - Yang, Jiajia - Zhang, Jianwu - Yue, Hengli	2018

Con los artículos seleccionados, se empleó el software VOSViewer, con el cual se identificó las palabras claves más predominantes, entre los artículos seleccionados, se escogió un mínimo de 2 ocurrencias por palabra clave. En la figura 1, se muestran las diferentes palabras, con predominio de *Biometric authentication, authentication* y *biometrics* entre los diferentes artículos.

Figura 1

Gráfico VOSViewer con las palabras claves



De los artículos elegidos, se identificó un conjunto de beneficios que trae la tecnología biométrica en la autenticación de usuarios, de los beneficios identificados en los artículos, se presenta en la Tabla 3, los beneficios más relevantes encontrados.

Es necesario recalcar que, en los artículos analizados, se encontró que la tecnología biométrica más utilizada en la mayoría de aplicaciones de alta seguridad es el reconocimiento de retina, ya que la retina tiene una disposición única de sus cuatro capas que la componen, también al ser una zona sensible del cuerpo humano es muy difícil que se pueda replicar.

Tabla 3
Lista de beneficios de la tecnología biométrica

N.°	Beneficios	Artículos	Total
1	Aumento de seguridad del control de acceso de usuarios.	(Zhou & Ren, 2018), (Altuwayjiri et al., 2022), (Albalawi et al., 2022), (El-El-Sofany, 2022), (El-Gazar et al., 2022), (Bharath & Radhakrishna Rao, 2022), (Zhang et al., 2022), (Park & Kim, 2022), (Jaswal et al., 2021), (Laka et al., 2021), (Chin et al., 2021), (Parkinson et al., 2021), (Zhu & Cao, 2021), (Kovalan et al., 2021), (Kausar, 2020), (Wu et al., 2018)	16
2	Ahorro de esfuerzo y tiempo al no tener que recordar una contraseña.	(Kao & Chueh, 2023), (Albalawi et al., 2022), (El-El-Sofany, 2022), (Zhang et al., 2022), (Laka et al., 2021), (Parkinson et al., 2021), (Gehrmann et al., 2019), (Lee et al., 2019), (Arun & Sudhakar, 2019)	9
3	Fácil adaptación de las personas al nuevo proceso de autenticación.	(Kao & Chueh, 2023), (El-El-Sofany, 2022), (Bharath & Radhakrishna Rao, 2022), (Zhang et al., 2022), (Laka et al., 2021), (Chin et al., 2021), (Alhayajneh et al., 2018)	7
4	Reducción de costes en la emisión de tarjetas de identificación.	(Kao & Chueh, 2023), (Albalawi et al., 2022), (El-El-Sofany, 2022), (Laka et al., 2021), (Chin et al., 2021), (Salem et al., 2019)	6
5	Aumenta la privacidad al incrementar la seguridad en la transmisión de datos personales.	(Zhou & Ren, 2018), (Albalawi et al., 2022), (El-El-Sofany, 2022), (El-Gazar et al., 2022), (Zhang et al., 2022)	5

4. Discusión

Los resultados obtenidos respecto a los beneficios que generan las tecnologías biométricas en la autenticación de usuarios, muestran que el beneficio más significativo es el aumento de la seguridad del control de acceso, esto coincide con lo mencionado por Albalawi et al. (2022) que indica que esta tecnología es adecuada para las aplicaciones que requieran de alta seguridad; también El-El-Sofany (2022) sugiere que dado que las características de cada persona son únicos para todos, la autenticación biométrica es mucho más segura que las formas tradicionales.

Zhang et al. (2022) indican que la autenticación biométrica ahorra el esfuerzo al no requerir que los usuarios recuerden ninguna contraseña, al igual que permite estar realizar otras actividades mientras se puede realizar la autenticación por medios biométricos.

La mayoría de los servicios en línea todavía utilizan usuarios y contraseñas, este método de autenticación de usuarios tienen varios problemas de seguridad, como una gestión deficiente de contraseñas, y si la contraseña es segura, es difícil de recordar, por tal razón los usuarios utilizan contraseñas fáciles de predecir. Debido al cual, una alternativa más fácil de usar es la autenticación biométrica como forma de autenticación de usuarios al iniciar sesión (Gehrmann et al., 2019).

La autenticación biométrica se utiliza de manera amplia en la autenticación inalámbrica, pero aún tiene problemas de precisión limitada o suplantación por esta, por lo que Wu et al. (2018) proponen la implementación de tecnología biométrica multibiométrica con una fusión de huella dactilar por su alta estabilidad y huella de voz por la aceptación que tiene está por los usuarios, con el objetivo de aumentar la precisión al realizar la autenticación del usuario, y poder aumentar la seguridad del control de acceso y la preservación de la privacidad.

Los algoritmos de aprendizaje automático basado en redes neuronales, sobre los que están hechos algunos de los sistemas de autenticación biométrica, son vulnerables a los ataques de adversarios, con el uso de ataques contra estos sistemas se logra reducir en gran medida la precisión del sistema, generando que este funcione con menor precisión y no logre efectuar la autenticación del usuario de forma correcta (Usoltsev et al., 2022).

También existen otra forma de vulnerar esta tecnología, por ejemplo, la información de biometría utilizada en los portátiles se almacena en el dispositivo portátil por lo que puede ser robado y esa información puede ser alterada, también en los portátiles, los sensores son de un tamaño más limitado por lo que la calidad de la información es más baja (Lee et al., 2019), en consecuencia se debe de tener cuidado con los dispositivos en los que se almacena información importante.

Como se puede apreciar en el párrafo anterior, aunque exista mucha más seguridad haciendo uso de la tecnología biométrica, aún existen formas de vulnerarla, por lo que las futuras líneas de investigación deberían estar enfocadas sobre cómo hacer frente a estas vulnerabilidades y en como disminuir o eliminar estas, así como sería recomendable el de publicar estas investigaciones con acceso libre para el lector.

5. Conclusiones

Se concluye que la tecnología biométrica está tomando cada día más impulso en la autenticación de usuarios por los beneficios que este trae, y que se está perfeccionando cada vez más para hacerla más precisa y mucho más difícil de vulnerar.

Por otro lado, se llegó a la conclusión que la autenticación de usuarios mediante tecnologías biométricas, tiene como beneficios más relevantes, el aumento de la seguridad al realizar el control de acceso de los usuarios y el ahorro de esfuerzo y tiempo al no tener que recordar una contraseña, porque la autenticación se hace con las características del mismo cuerpo, lo que genera que sea mucho más difícil de falsificar; también, se llegó a la conclusión que es mejor implementar más de un tipo de autenticación biométrica para que se tenga así mayor seguridad y evitar que se realicen suplantaciones.

Si bien es cierto que los beneficios que trae la tecnología biométrica para la realización de autenticación de usuarios, también se encuentra que la mayor desventaja de estas

tecnologías es su precisión al ejecutar la autenticación, por lo que se sugiere seguir ampliando sobre el tema en las futuras investigaciones.

6. Referencias Bibliográficas

Albalawi, S., Alshahrani, L., Albalawi, N., Kilabi, R., & Alhakamy, aeshah. (2022). A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 13, Issue 4). www.ijacsa.thesai.org

Alhayajneh, A., Baccarini, A. N., Weiss, G. M., Hayajneh, T., & Farajidavar, A. (2018). Biometric authentication and verification for medical cyber physical systems. *Electronics (Switzerland)*, *7*(12). https://doi.org/10.3390/electronics7120436

Altuwayjiri, S. M., Bchir, O., Maher, M., & Ismail, B. (2022). Mining Hidden Partitions of Voice Utterances using Fuzzy Clustering for Generalized Voice Spoofing Countermeasures. In IJACSA) International Journal of Advanced Computer Science and Applications (Vol. 13, Issue 5). www.ijacsa.thesai.org

Arun, V., & Sudhakar, R. (2019). User behavioral analysis using Markov chain and steady-state in tracer and checker model. Journal of Cyber Security and Mobility, 8(2), 277–294. https://doi.org/10.13052/JCSM2245-1439.826

Bharath, M. R., & Radhakrishna Rao, K. A. (2022). A novel multimodal hand database for biometric authentication. International Journal of Advanced Technology and Engineering Exploration, 9(86), 127–142. https://doi.org/10.19101/IJATEE.2021.874525

Chin, S. W., Tay, K. G., Chew, C. C., Huong, A., & Rahim, R. A. (2021). Dorsal hand vein authentication system using artificial neural network. Indonesian Journal of Electrical Engineering and Computer Science, 21(3), 1837–1846. https://doi.org/10.11591/ijeecs.v21.i3.pp1837-1846

El-El-Sofany, H. (2022). A Proposed Biometric Authentication Model to Improve Cloud Systems Security. Computer Systems Science and Engineering, 43(2), 573–589. https://doi.org/10.32604/csse.2022.024302

El-Gazar, S., El-Shafai, W., El-Banby, G., Hamed, H. F. A., Salama, G. M., Abd-Elnaby, M., & Abd El-Samie, F. E. (2022). Cancelable Speaker Identification System Based on Optical-Like Encryption Algorithms. Computer Systems Science and Engineering, 43(1), 87–102. https://doi.org/10.32604/csse.2022.022722

Gehrmann, C., Rodan, M., & Jönsson, N. (2019). Metadata filtering for user-friendly centralized biometric authentication. Eurasip Journal on Information Security, 2019(1). https://doi.org/10.1186/s13635-019-0093-3

Jaswal, G., Bharadwaj, R., Tiwari, K., Thapar, D., Goyal, P., & Nigam, A. (2021). AI-Biometric-Driven Smartphone App for Strict Post-COVID Home Quarantine Management. IEEE Consumer Electronics Magazine, 10(3), 49–55. https://doi.org/10.1109/MCE.2020.3039035

Kao, C. Y., & Chueh, H. E. (2023). Voice Response Questionnaire System for Speaker Recognition Using Biometric Authentication Interface. Intelligent Automation and Soft Computing,

35(1), 913–924. https://doi.org/10.32604/iasc.2023.024734

Kausar, F. (2020). Cancelable Face Template Protection using Transform Features for Cyberworld Security. In IJACSA) International Journal of Advanced Computer Science and Applications (Vol. 11, Issue 1). www.ijacsa.thesai.org

Kovalan, K., Zobidah Omar, S., Tang, L., Bolong, J., Abdullah, R., Hayati Ahmad Ghazali, A., & Adnan Pitchan, M. (2021). A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users. In IJACSA) International Journal of Advanced Computer Science and Applications (Vol. 12, Issue 7). www.ijacsa.thesai.org

Laka, P., Korzeb, Z., & Mazurczyk, W. (2021). Novel user authentication method based on body composition analysis. Telecommun, 76, 175–185. https://doi.org/10.1007/s12243-020-00779-y/Published

Lee, S., Jeong, I. R., & Araujo, A. (2019). A Cancelable Template for the Low-Quality Fingerprints from Wearable Devices. Security and Communication Networks, 2019. https://doi.org/10.1155/2019/4202671

Park, H., & Kim, T. (2022). User Authentication Method via Speaker Recognition and Speech Synthesis Detection. Security and Communication Networks, 2022. https://doi.org/10.1155/2022/5755785

Parkinson, S., Khan, S., Crampton, A., Xu, Q., Xie, W., Liu, N., & Dakin, K. (2021). Password policy characteristics and keystroke biometric authentication. IET Biometrics, 10(2), 163–178. https://doi.org/10.1049/bme2.12017

Real Academia Española. (2014). Diccionario de la Lengua Española (23a ed.).

Salem, A., Sharieh, A., Sleit, A., & Jabri, R. (2019). Enhanced authentication system performance based on keystroke dynamics using classification algorithms. KSII Transactions on Internet and Information Systems, 13(8), 4076–4092. https://doi.org/10.3837/tiis.2019.08.014

Usoltsev, Y., Lodonova, B., Shelupanov, A., Konev, A., & Kostyuchenko, E. (2022). Adversarial Attacks Impact on the Neural Network Performance and Visual Perception of Data under Attack. Information (Switzerland), 13(2). https://doi.org/10.3390/info13020077

Wu, Z., Yang, J., Zhang, J., & Yue, H. (2018). Multibiometric Fusion Authentication in Wireless Multimedia Environment Using Dynamic Bayesian Method. Security and Communication Networks, 2018. https://doi.org/10.1155/2018/5783976

Zhang, R., Yan, Z., Wang, X., & Deng, R. (2022). VOLERE: Leakage Resilient User Authentication Based on Personal Voice Challenges. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2022.3147504

Zhou, K., & Ren, J. (2018). Comments on "PassBio: Privacy-preserving user-centric biometric authentication." IEEE Transactions on Information Forensics and Security, 13(12), 3050–3063. https://doi.org/10.1109/TIFS.2018.2838540

Zhu, X., & Cao, C. (2021). Secure Online Examination with Biometric Authentication and Blockchain-Based Framework. *Mathematical Problems in Engineering*, *2021*. https://doi.org/10.1155/2021/5058780