Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Revisión sistemática de la literatura sobre métodos de autenticación biométrica en aplicaciones móviles.

Systematic literature review on biometric authentication methods in mobile applications.

Gabriela Stephania Bailón Zambrano, David Fernando Zambrano Montenegro.

CIENCIA E INNOVACIÓN EN DIVERSAS DISCIPLINAS CIENTÍFICAS.
Julio - Diciembre, V°5-N°2; 2024

- ✓ **Recibido:** 05/09/2024
- ✓ **Aceptado**: 16/09/2024
- ✓ **Publicado:** 31/12/2024

PAIS
Portoviejo, Ecuador.
Manta, Ecuador.

INSTITUCION
- Universidad Técnica de Manabí
- Universidad Técnica de Manabí

CORREO:
gbailon9422@utm.edu.ec
david.zambrano@utm.edu.ec

ORCID:
https://orcid.org/0009-0008-2616-8596
https://orcid.org/0000-0002-8833-1546

FORMATO DE CITA APA.
Bailón, G. Zambrano, D. (2024). Revisión sistemática de la literatura sobre métodos de autenticación biométrica en aplicaciones móviles. G-ner@ndo, V°5 (N°2,).1233 – 1258.

Resumen

La investigación se basa en una revisión sistemática de la literatura (RSL) siguiendo la metodología de Kitchenham y Charters, y se estructura en tres fases: planificación, ejecución y análisis de resultados. El estudio aborda tres preguntas de investigación: los tipos de métodos utilizados, las vulnerabilidades específicas y las tendencias futuras. Los resultados indican una prevalencia de métodos como el reconocimiento facial, las huellas dactilares y la voz, siendo estos los más adoptados en aplicaciones financieras. Se identificaron vulnerabilidades, tales como ataques de suplantación y problemas de precisión relacionados con factores ambientales. Aunque los métodos biométricos son generalmente más seguros que las contraseñas tradicionales, también presentan riesgos de spoofing e intercepción de datos. Las tendencias futuras en la investigación incluyen la integración de múltiples modalidades biométricas, el desarrollo de algoritmos avanzados y la mejora de la usabilidad.

Palabras clave: Autenticación biométrica, Métodos biométricos, Seguridad en aplicaciones móviles.

Abstract

The research is based on a systematic literature review (SLR) following the Kitchenham and Charters methodology, and is structured in three phases: planning, execution and analysis of results. The study addresses three research questions: the types of methods used, specific vulnerabilities and future trends. The results indicate a prevalence of methods such as facial recognition, fingerprints and voice, these being the most widely adopted in financial applications. Vulnerabilities were identified, such as spoofing attacks and accuracy issues related to environmental factors. Although biometric methods are generally more secure than traditional passwords, they also present risks of spoofing and data interception. Future trends in research include the integration of multiple biometric modalities, the development of advanced algorithms and the improvement of usability.

Keywords: Biometric authentication, Biometric methods, Security in mobile applications.

Introducción

En la actualidad, la biometría se emplea en una amplia gama de aplicaciones, como el cumplimiento de la ley, aplicaciones comerciales, billeteras digitales, servicios de salud, banca móvil, control migratorio, entre otras. Estas aplicaciones emplean diversos métodos de autenticación biométrica, los cuales se basan en los atributos físicos o de comportamiento característicos de un individuo (Karakaya et al., 2019). Estos métodos se pueden clasificar en dos categorías: biometría fisiológica y biometría conductual. La biometría fisiológica es una característica física relacionada con los rasgos estáticos de un cuerpo humano que no están sujetos a cambios con el envejecimiento. Por otro lado, la biometría conductual se enfoca en los rasgos de comportamiento de un individuo (Ananthio et al., 2023)

Las ventajas de ambos métodos biométricos son evidentes en términos de seguridad, ya que ofrecen una forma única y difícil de suplantar la identidad de un usuario. Estos métodos mejoran la experiencia del usuario al proporcionar un acceso rápido y sin esfuerzo a sus aplicaciones. Sin embargo, debido a la diversidad de las aplicaciones biométricas, es poco probable que un solo rasgo biométrico sea óptimo y satisfaga por completo los requisitos de todas las aplicaciones (Alwahaishi & Zdralek, 2020)

A pesar de sus ventajas, las aplicaciones móviles que utilizan métodos biométricos presentan ciertas vulnerabilidades. Surgen preocupaciones sobre la privacidad y el manejo seguro de la información biométrica. Además, la experiencia del usuario puede verse afectada por diversos factores. Por un lado, existen vulnerabilidades asociadas a cambios físicos, como daños en los dedos o alteraciones faciales, que pueden comprometer la eficacia de la autenticación(Ananthio et al., 2023). Por otro lado, factores ambientales como la iluminación, el ruido o la humedad pueden influir en la precisión del sistema, generando inconvenientes en su uso cotidiano (Albalawi et al., 2022). Las tendencias futuras en investigación se centran en el desarrollo de nuevas modalidades biométricas y en la mejora de las ya existentes. Por ejemplo, patrones de venas es un método biométrico prometedora que podría proporcionar mayor

seguridad en la autenticación(Ayeswarya & Singh, 2024) . Además, se trabaja en la integración de múltiples modalidades biométricas para crear sistemas de autenticación más robustos y adaptables. Paralelamente, surge una mayor necesidad de establecer marcos regulatorios que garanticen la protección de los datos personales y limiten el uso indebido de la información biométrica.

El objetivo principal de esta revisión sistemática es conocer el estado actual de las aplicaciones móviles que utilizan métodos de autenticación biométrica, identificando los tipos de métodos empleados, sus vulnerabilidades, así como las tendencias de investigación futura en este campo.

El trabajo de Estrela (2020), abarca sobre autenticación continua en aplicaciones de banca móvil basado en biometría conductual, detallan varios resultados obtenidos a partir de los experimentos realizados. En general, los resultados mostraron una precisión media entre 78% y 91%, lo que valida la efectividad potencial de la biometría comportamental touch en combinación con métodos tradicionales como contraseñas para la seguridad en aplicaciones bancarias móviles.

Jaswal (2021), propone una aplicación móvil llamada "LakshmanRekha" que utiliza técnicas de inteligencia artificial, biometría facial y geolocalización para garantizar un estricto cumplimiento de la cuarentena domiciliaria en post-COVID. La aplicación combina la autenticación biométrica continua (CUBA) con el geofencing para monitorear constantemente la identidad y ubicación del usuario, evitando así que los pacientes en cuarentena violen las reglas entre intervalos de tiempo.Por otra parte, Jeon (2019), habla sobre un desarrollo de una aplicación móvil de reconocimiento facial para la identificación de pacientes con una precisión del 99%. La aplicación pudo reconocer e identificar correctamente a pacientes ambulatorios y hospitalizados, incluso cuando los pacientes estaban inconscientes bajo anestesia. La aplicación permite un proceso de identificación de pacientes rápido, simple y sin contacto físico,

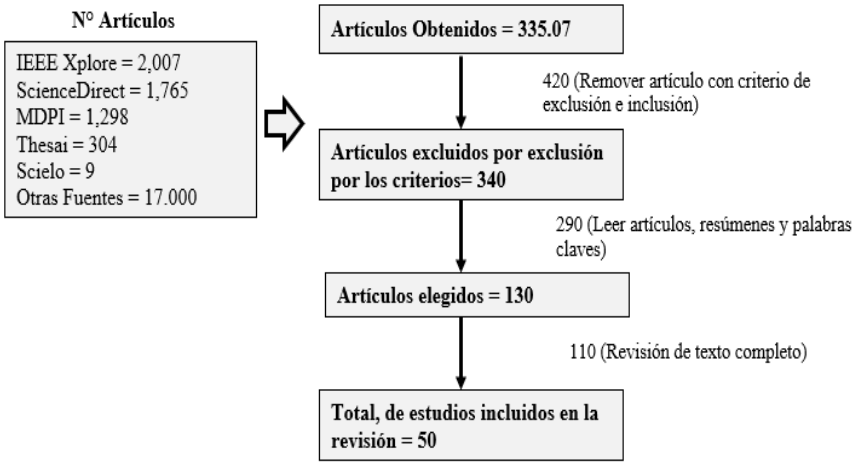
superando las limitaciones de otros métodos biométricos como escáneres de huellas dactilares o iris que requieren contacto o que el paciente esté consciente.

La autenticación de usuarios se manifiesta en el proyecto de Incel (2021), que investiga la posibilidad de autenticar continuamente a los usuarios a través de la biometría de comportamiento en una aplicación de banca móvil. En este estudio, se recopilaron datos de 45 participantes utilizando la pantalla táctil y los sensores de movimiento del teléfono. Estos datos se utilizaron para entrenar siete algoritmos de clasificación, destacándose el SVM binario con kernel RBF, que logró la menor tasa de error, alcanzando un 3.5% de EER. En condiciones de prueba en tiempo real, el sistema DAKOTA logró una tasa promedio de reconocimiento verdadero del 90%, sin un impacto significativo en el consumo de recursos del dispositivo.

Materiales y Métodos

Esta revisión sistemática de la literatura (RSL) sigue la metodología propuesta por Kitchenham y Charter (*Guidelines for Performing Systematic Literature Reviews in Software Engineering*, 2007), que consta de tres fases: planificación, ejecución y análisis de resultados. La investigación se caracteriza por tener un enfoque documental y exploratorio.

Figura 1. *Flujo de búsqueda y selección de artículos.*



Los resultados de este estudio se destacan por su rigurosa selección y revisión de artículos. La investigación cumple con los criterios de verificación predefinidos, lo cual se evidencia claramente en la figura 1.

Planificación:

En esta fase, se establecen las preguntas de investigación que orientaron el estudio, se detallan las fuentes de datos consultadas para encontrar los artículos científicos y se explican los criterios de selección utilizados. Los objetivos de esta revisión se abordan a través de las siguientes preguntas de investigación:

RQ1: ¿Qué tipos de métodos de autenticación biométrica se están utilizando actualmente en aplicaciones móviles?

RQ2: ¿Existen vulnerabilidades específicas asociadas a cada método biométrico en aplicaciones móviles?

RQ3: ¿Cuáles son las tendencias futuras en la autenticación biométrica en aplicaciones móviles?

Para llevar a cabo una revisión sistemática sobre los diferentes métodos de autenticación biométrica utilizados en aplicaciones móviles, se realizó una búsqueda en diversas bases de datos académicas, como IEEE Xplore, ScienceDirect, MDPI, thesai, Scielo y otras fuentes relevantes del buscador Google academic. Con el fin de obtener resultados relevantes, se emplearon operadores booleanos como “AND” y “OR” para combinar diferentes términos de búsqueda relacionados con el tema de investigación. Las cadenas de búsqueda se adaptan a cada base de datos o motor de búsqueda, debido a las particularidades de la documentación disponible en cada plataforma (tabla 1). Los estudios seleccionados fueron revisados y evaluados según criterios de inclusión y exclusión predefinidos (tabla 2). Esta búsqueda sistemática se centró en estudios primarios publicados entre 2019 y 2024. Con la excepción del trabajo de Galterio (2018), que es esencial para analizar las vulnerabilidades de la aplicación móvil en el método biométrico.

Cadena de búsqueda: (“Autenticación Biométrica” OR “Métodos Biométricos” OR “Autenticación” OR “Biometría”) AND (“Aplicación Móvil”) AND (“Seguridad”).

Cadena de búsqueda según el gestor de base de datos académicas:

Tabla 1 Cadena de búsqueda usada para cada Base de Datos Académica.

Cadena de búsqueda	Base de datos académicas
(“Biometric Authentication” OR “Biometric Methods” OR “Authentication” OR “Biometrics”) AND (“Mobile Application”) AND (“Security”)	IEEE Xplore
(“Biometric Authentication” OR “Biometric Methods” OR “Authentication” OR “Biometrics”) AND (“Mobile Application”) AND (“Security”)	ScienceDirect
(“Biometric Authentication” OR “Biometric Methods” OR “Authentication” OR “Biometrics”) AND (“Mobile Application”) AND (“Security”) ("Biometric Authentication") AND ("Applications Mobile")	MDPI
(“Biometric Authentication” OR “Biometric Methods” OR “Authentication” OR “Biometrics”) AND (“Mobile Application”) AND (“Security”)	Thesai
("Biometric") AND ("Application mobile") (“Biometric”) AND (“Security”)	Scielo
(“Biometric Authentication” OR “Authentication” OR “Biometrics”) AND (“Mobile Application” OR “Mobile Device”) AND (“Security”). ("Biometric") AND ("Application mobile") (“Biometric Authentication”) AND (“Mobile Application”) AND (“Security”)	Otras fuentes

Fuente: Elaboración propia a partir de autor.

Para optimizar los procesos de búsqueda, se establecieron criterios detallados de inclusión y exclusión, los cuales se explican en la tabla 2. Estos criterios de selección facilitaron la identificación y selección de los documentos más relevantes para el estudio de la autenticación biométrica en aplicaciones móviles.

Tabla 2. Criterios de exclusión e inclusión

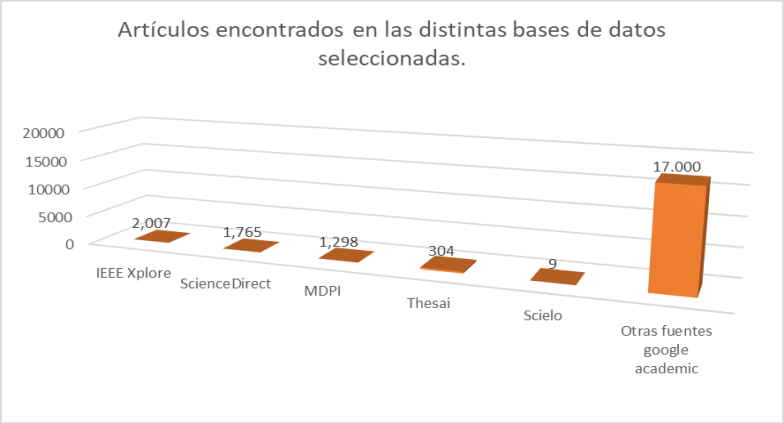
Criterios de Inclusión	Criterios de Exclusión
Artículo de revistas indexadas	Publicaciones en redes sociales, estudios duplicados, tesis. Estudios desactualizados

Fuente: *Elaboración propia a partir de autor*.

Revisión:

En la fase inicial de recopilación de datos, se consultaron diversas bases de datos. La Figura 2, ilustra las cifras obtenidas, las cuales representan una cantidad considerable de documentos pertinentes al tema de estudio procedentes de estas fuentes.

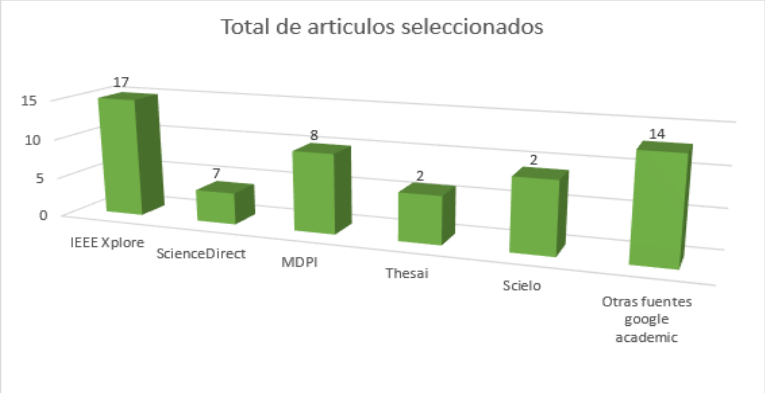
Figura 2. Artículos encontrados en las bases de datos seleccionadas.



Luego, se aplicaron los criterios de inclusión y exclusión diseñados para filtrar los artículos que no eran relevantes para el tema de estudio. El efecto de esta filtración se puede ver en la Figura 3. El número de documentos seleccionados se redujo: de IEEE se seleccionaron

17, de ScienceDirect 7, de MDPI 8, de Thesai 2, de Scielo 2 y de otras fuentes académicas buscadas en Google Scholar 14, dando un total de 50 documentos.

Figura 3. Artículos seleccionados después de la segunda revisión.



En este paso, se revisaron los estudios más relevantes para garantizar su utilidad en esta investigación. Se verificó que cada uno abordará métodos biométricos, áreas de investigación y vulnerabilidades en aplicaciones móviles, lo cual contribuirá a responder las preguntas de investigación (ver Tabla 3)

Tabla 3. *Clasificación de estudios primarios seleccionados según el área*

Base de datos	Autor(es)	Aplicación móvil	Área de aplicación
IEEE Xplore	(Jaswal et al., 2021)	Aplicaciones móviles post-COVID	Métodos biométricos.
ScienceDirect	(Basar et al., 2019)	Aplicaciones móviles de pago en el análisis del consumo de recursos	Vulnerabilidades.
MDPI	(Medvedev et al., 2021) (Estrela et al., 2021)	Aplicaciones móviles de seguridad de documentos. Aplicación móvil bancaria.	Área de investigación. Métodos biométricos, vulnerabilidades, área de investigación.

Thesai	(Hassan et al., 2020)	Aplicación móvil capaz de leer código QR	Métodos biométricos.
Scielo	(Rivero Albarrán et al., 2023)	Aplicación móvil CRM Comercial de la empresa ChevyPlan.	Métodos biométricos
Otras fuentes del buscador Google academic	(Algarni, 2023)	Aplicación móvil Android	Método biométrico, vulnerabilidades.

Fuente: *Elaboración propia a partir de autor.*

Análisis de Resultados

RQ1: ¿Qué tipos de métodos de autenticación biométrica se están utilizando actualmente en aplicaciones móviles?

En términos generales (Ryu et al., 2021), destaca la combinación dominante de métodos biométricos, como la dinámica de pulsaciones, perteneciente a la categoría conductual y el reconocimiento facial, de categoría fisiológica. Esta predominancia se debe a que ambos no requieren dispositivos adicionales, pues la mayoría de los sistemas ya cuentan con un teclado y una cámara integrados. Por otra parte, se ha observado un gran interés en otras modalidades biométricas, como los gestos táctiles, las huellas dactilares y el reconocimiento de voz, lo cual coincide con el aumento en el uso de aplicaciones móviles. Actualmente, existe una amplia variedad de métodos de autenticación biométrica disponibles para aplicaciones móviles. Por ello, la tabla 4 recopila los resultados de varios estudios, analizando, mostrando los métodos biométricos más frecuentes en aplicaciones móviles.

Tabla 4. *Tipos de autenticación biométrica en aplicaciones móviles.*

ID	Autenticación biométrica	Aplicación móvil	Referencia

1	Reconocimiento facial utilizado por ciones como "Hogar-cuarentena" en a, que recoge selfies aleatorias de los os. Autenticación biométrica continúa ada con geofencing para un monitoreo stricto del cumplimiento de la cuarentena. Reconocimiento facial Huella dactilar, este método se utiliza plicaciones móviles del usuario por os que no requieran tocar una superficie emia de COVID-19)	Aplicaciones móviles COVID. Aplicación "CUBA-HQM". Aplicación de salud móvil eguridad del paciente. Aplicación de Android que a continuamente imágenes dos para el reconocimiento ellas dactilares.	(Jaswal et al., 2021) (Jeon et al., 2019), nitz et al., 2022)
2	Voz, los usuarios graban su plantilla de través de esa aplicación.	Aplicación móvil PIDaaS dad Privada como io)	(Blanco-Gonzalo et 19)
3	Huella dactilar	Aplicaciones móviles es de leer códigos QR, nejorar el pago electrónico.	(Hassan et al., 2020)
4	Huella dactilar y autenticación por imiento (contraseña)	Aplicación móvil CRM rcial de la empresa Plan.	(Rivero Albarrán et 23)

5	Huella dactilar	Aplicación móvil para id, mejorar la seguridad de usar aplicaciones.	(Algarni, 2023)
6	Huella dactilar Iris Voz Reconocimiento Facial Retina Autenticación continúa utilizando tría conductual (Datos de sensores: ómetro, giroscopio, magnetómetro y de pantalla táctil) Autenticación biométrica a mano Reconocimiento facial basado en dizaje profundo	Aplicación de dinero móvil Aplicación móvil M-pesa Aplicación de pago móvil Banca móvil Aplicaciones en cciones en línea (Banca, ra, Compra) Aplicaciones de pago (comercio minorista, rantes y modelos de ios hoteleros) Aplicación de banca móvil rid) Aplicación banca móvil KOTA) Usuario de aplicación móvil Aplicación de banca móvil Aplicaciones financieras s de bancos y FinTech.	(Ali et al., 2021) (Ali et al., 2020) (Islam et al., 2019) (Sharma et al., 2019) (Dijmarescu et al., (Basar et al., 2019) (Ximenes et al., (Shuhidan et al., (Incel et al., 2021) (Estrela et al., 2020) (Prihodova & Hub, (Yildirim & Varol, (Machap Marco, (Liébana-Cabanillas 2024)

			(Piotrowska, 2024) (Barlas et al., 2020) (Kumari, 2024)
7	Sistema de autenticación sin señas, diseñada para funcionar en itivos Android e iOS, sus métodos de icación son: Huellas dactilares o ocimiento facial.	Sesame Auth (SA)	(Oduguwa & Arabo,
8	Facial y Voz	Aplicación móvil Android, realizar autenticación de lad.	(Zhang et al., 2020)
9	Huella dactilar Gestos dactilares Voz	Aplicaciones móviles para itivos inteligentes	(Ryu et al., 2021)
10	Comportamiento táctil	TouchMetric, para probar os de aprendizaje ático	(Samet et al., 2019)
11	Autenticación multifactor Biométrico a digital) y contraseña (clave de inicio de)	Aplicación de servidor de lo cliente en un entorno	(Kovalan et al.,

12	Facial	Aplicación de Android que e datos importantes nte biometría.	(Anbalagan et al.,
13	Firmas manuscritas	Aplicación móvil para icar la firma directamente.	(Fakhiroh et al.,
14	Facial	Aplicación móvil MySIMS ada a pequeñas ciones educativas.	(Othman et al., 2024)
15	Facial	Aplicación móvil Android el reconocimiento de o, edad y rostro	(Salihbašic & vacki, 2019)
16	Facial	Aplicación móvil de ncia para estudiantes	(Sunaryono et al.,

RQ2: ¿Existen vulnerabilidades específicas asociadas a cada método biométrico en aplicaciones móviles?

Los métodos de autenticación biométrica fisiológica, aunque inicialmente considerados seguros, han demostrado ser vulnerables a ataques de suplantación. Investigadores han evidenciado que estos métodos pueden ser comprometidas con cierta facilidad. A diferencia de los métodos de biometría conductual se consideran más seguros, ya que se basan en patrones de comportamiento únicos que no pueden ser copiados, perdidos o robados con la misma facilidad que los rasgos físicos. Sin embargo, es importante reconocer que ningún método de

autenticación es completamente seguro. La Tabla 5 presenta un resumen de estudios recientes sobre

vulnerabilidades identificadas en aplicaciones móviles, ilustrando la diversidad de las amenazas actuales en autenticación biométrica.

Tabla 5. *Vulnerabilidades en aplicaciones móviles con su método biométrico.*

D	**Aplicación Móvil**	**Vulnerabilidad**	**Referencia**
	Sistemas de reconocimiento facial	Estos sistemas enfrentan amenazas de ataques de presentación, donde se busca suplantar la identidad del usuario o engañar al sistema	(Medvedev et al., 2021)
	FaceLock (Android) AppLock (Android) Luxand Face Recognition (Android y iOS) True Key (Android y iOS) BioID Facial Recognition (iOS)	Fue engañada por fotos impresas y electrónicas, por videos del usuario autorizado Esta fue la app más vulnerable, pudiendo ser engañada por fotos impresas y electrónicas, videos, e incluso por una persona con características faciales similares Aunque fue la más segura, tuvo problemas para identificar correctamente al usuario autorizado y pudo ser engañada por fotos impresas con lentes de contacto Mostró vulnerabilidades diferentes en Android e iOS. En Android, fue engañada por fotos impresas, mientras que en iOS fue engañada por fotos electrónicas y videos. Fue engañada por videos del usuario autorizado y por alguien que se parecía al usuario autorizado	(Galterio et al., 2018)
	Dinero móvil	M-pesa, biometría voz,puede cambiar con el tiempo lo cual puede generar algunos errores en el reconocimiento PYME, iris, las gafas pueden reducir la calidad de la imagen del iris y el rendimiento Huella dactilar, vulnerabilidad a suplantación de identidad, datos biométricos digitales falsos,	(Ali et al., 2021)

		ataque de caballo de troya, coincidencia, repetición e intrusión.	
	Aplicaciones móviles en la transacción de dinero	La posibilidad de duplicación de datos biométricos representa un riesgo. Si no se manejan adecuadamente, los datos biométricos, como las huellas digitales o el reconocimiento facial, pueden ser replicados o clonados.	(Khan et al., 2023)
	Aplicación de Android que captura continuamente imágenes de dedos	Reconocimiento de huellas dactilares (Pandemia COVID-19). Las condiciones ambientales pueden afectar la precisión de la captura y el procesamiento de las huellas dactilares, lo que puede resultar en imágenes borrosas o segmentaciones incorrectas	(Priesnitz et al., 2022)
	Método BehaveSense, implementado en la aplicación móvil WeChat, el cual es una aplicación de mensajería y redes sociales muy popular en China, que también incluye funcionalidades de pago móvil.	El sistema requiere un monitoreo continuo de las interacciones del usuario, lo que podría plantear preocupaciones de privacidad para algunos usuarios. Aunque la precisión es alta, todavía existe un margen de error que podría resultar en falsos rechazos (negando el acceso al propietario legítimo) o falsos aceptos (permitiendo el acceso a un impostor)	(Yang et al., 2019)
	Aplicaciones móviles para transacciones en línea como banca, billeteras y compras.	Los patrones de voz pueden cambiar, lo que podría afectar la precisión del reconocimiento. Para las huellas dactilares, señala como desventaja que si se roban son pérdidas permanentes.	(Sharma et al., 2019)
	Aplicación móvil (pago móvil)	Hay una gran preocupación por la privacidad y el almacenamiento seguro de estos datos, ya que, a diferencia de las contraseñas, no se pueden cambiar una vez que han sido comprometidos. Además, factores físicos como daños a las características biométricas, como cortes en los dedos o cambios faciales debido a accidentes, pueden dificultar la autenticación y causar	(Morake et al., 2021)

		inconvenientes a los usuarios. Algunas personas, especialmente aquellas menos familiarizadas con la tecnología, pueden preferir los métodos tradicionales de contraseñas o PINs.	
	Aplicación banca móvil	Los sistemas de reconocimiento biométrico desarrollados para dispositivos móviles necesitan ser integrados y utilizados adecuadamente en las aplicaciones de banca móvil, ya que puede ver vulnerabilidades de implementación.	(Yildirim & Varol, 2019)
0	Aplicaciones Android Aplicación de pago móvil con más de 100 millones de instalaciones	Muchas aplicaciones solo cancelan la autenticación de huella dactilar en el evento onStop en lugar de onPause, lo que las hace vulnerables a ataques. Contiene el fallo de "pause-failure", lo que la hace vulnerable a la mayoría de los ataques de "fingerprint-jacking" El proceso de pago de la aplicación puede ser invocado externamente desde otra aplicación o incluso desde una página web. Debido a esta vulnerabilidad, es posible realizar un robo de dinero iniciando pagos no autorizados a sus propias cuentas y engañando a las víctimas para que los autoricen con su huella dactilar	(Wang et al., 2020)
1	Aplicación móvil para proteger biometría	El reconocimiento facial, puede fallar debido a factores ambientales como iluminación y ángulos de captura inadecuados.	(Anbalagan et al., 2020)
2	Aplicación móvil para pagar facturas	El reconocimiento facial, estos sistemas de autenticación, son vulnerables a robos y estafas, lo que expone a los usuarios al riesgo de ser víctimas de fraudes.	(Chandran & Chandran, 2022)

RQ3: ¿Cuáles son las áreas de investigación futuras en la autenticación biométrica en aplicaciones móviles?

La autenticación biométrica en aplicaciones móviles es un campo en rápida evolución que busca mejorar la seguridad y experiencia de usuario. Con el creciente uso de las aplicaciones moviles para transacciones financieras, atención médica y otras funciones críticas, la investigación en este campo se enfoca en dar una prospectiva de relevante evolución para aquellos interesados en la intersección entre tecnología, seguridad y experiencia de usuario. Algunos de los principales los trabajos de investigación futura identificados por diversos autores:

Roszczewska (2024), en su estudio abarca sobre una aplicación móvil de verificación de firmas basada en redes neuronales convolucionales (CNN) para dispositivos móviles. Destaca cómo esta integración mejora la autenticación de documentos. El área de investigación se centra en la autenticación biométrica conductual, en la verificación de firmas manuscritas en línea para aplicaciones móviles. Los autores planean expandir su investigación entrenando modelos con conjuntos de datos más diversos, explorando diferentes arquitecturas de CNN, y comparando sus resultados con otras soluciones existentes. Además, consideran crear un conjunto de datos que incluya falsificaciones generadas para entrenar modelos más robustos, lo que sugiere un enfoque en mejorar la detección de firmas falsificadas en entornos móviles.

Algarni (2023), su área de investigación futura se centra en la mejora de la seguridad de las aplicaciones de Android mediante la integración de diversas modalidades de autenticación. Además de la autenticación por huellas dactilares, se investigará la incorporación del reconocimiento facial y las técnicas de autenticación por voz, buscando cómo estos métodos pueden complementarse eficazmente para reforzar las medidas de seguridad. Asimismo, se dará prioridad a la usabilidad y la experiencia del usuario, realizando estudios que recojan sus aportaciones, mejorando la interfaz y optimizando el proceso de inscripción. Todo esto con el objetivo de asegurar un sistema amigable y fácil de usar. Finalmente, se verificará la tolerancia

del sistema hacia la escalabilidad y la compatibilidad, garantizando un rendimiento óptimo en una amplia gama de dispositivos Android.

Los autores destacan, que casi 2 mil millones de personas utilizan aplicaciones móviles para pagar sus facturas, y millones se suman a diario. Como área de investigación Chandran (2022), dice que es necesario realizar más estudios para desarrollar soluciones confiables que integren la tecnología blockchain con la autenticación de voz basada en inteligencia artificial. También será fundamental establecer protocolos y controles aceptables para todas las partes interesadas a nivel mundial.

Dijmarescu (2022), su área de investigación futura busca profundizar el conocimiento sobre la autenticación biométrica por reconocimiento facial como tecnología de pago móvil, explorando sus aplicaciones en diferentes entornos y mejorando los sistemas y algoritmos subyacentes. Por otra parte Estrela (2021), en su estudio propone ampliar la investigación mediante pruebas de campo en aplicaciones bancarias reales, con una mayor muestra de usuarios y duración. Se plantea analizar la relación entre modelos de teléfonos y calidad de datos de sensores, explorar métodos de selección adaptativa y técnicas avanzadas de ingeniería de características, e implementar filtros de datos para mejorar el rendimiento. Además, se sugiere profundizar en algoritmos de aprendizaje automático, comparar métodos de autenticación biométrica fisiológica y conductual, y fortalecer la resiliencia contra ataques mediante el estudio de modelos adversarios.

La aplicación móvil de reconocimiento facial de Jeon (2019) se desarrolló para verificar pacientes en hospitales. Incluye cinco módulos clave: registro, registros médicos, exámenes, recetas y citas. Como área de investigación futura se requiere investigación para mejorar la sensibilidad a la luz, evaluar con precisión el rendimiento en verificación de pacientes e integrar la aplicación con el sistema EMR del hospital.

Discusión.

Según Abazi (2019), la biometría es una de las herramientas de autenticación más efectivas, ya que se basa en características humanas únicas. En los métodos de autenticación biométrica utilizados actualmente en aplicaciones móviles, se observa que la diversidad de métodos es relevante, abarcando desde el reconocimiento facial y la huella dactilar hasta métodos más avanzados como la autenticación por voz, iris y retina. El presente estudio identificó 34 referencias que utilizan diversos métodos en aplicaciones móviles, revela que no existe un método único, sino una adaptación según los requisitos específicos de cada aplicación.

Entre los métodos analizados, la huella dactilar se destaca por su frecuente aparición en múltiples estudios, lo que indica su continua popularidad y su singularidad en cada individuo (Al Rousan & Intrigila, 2020). Este método de categoría fisiológica es uno de los más comunes (Hassan et al., 2020) y también el más antiguo (Albalawi et al., 2022), ya que ofrece una mayor seguridad, proporcionando a los usuarios una verificación más rápida (Morake et al., 2021)

Se observa una mayor adopción de métodos biométricos en aplicaciones móviles, destacando especialmente en el sector financiero. Las aplicaciones de banca, billeteras electrónicas y otras relacionadas con el ámbito financiero lideran con 17 referencias, empleando diversos métodos biométricos tanto fisiológicos como conductuales. Entre los métodos fisiológicos más utilizados se encuentran la huella dactilar, el reconocimiento facial, mientras que los conductuales aprovechan datos de sensores como el acelerómetro, el giroscopio, el magnetómetro y la información de la pantalla táctil. En segundo lugar, las aplicaciones de salud, con 3 referencias, han ganado importancia, especialmente durante la pandemia de COVID-19, utilizando reconocimiento facial, autenticación biométrica continúa mejorada con geofencing y huella dactilar. Otras aplicaciones móviles, resaltan su método biométrico y entre lo más usado son: huella dactilar, reconocimiento facial, reconocimiento de voz.

En el análisis de las vulnerabilidades asociadas a los métodos biométricos en aplicaciones móviles, como la huella dactilar, el reconocimiento de voz y facial, se destacan importantes preocupaciones de seguridad. Los sistemas de reconocimiento facial, como los utilizados en aplicaciones como Applock para Android, son particularmente susceptibles a ataques de presentación. Esta aplicación ha demostrado ser extremadamente vulnerable, pudiendo ser engañada no solo por fotografías impresas y electrónicas, sino también por videos y, en algunos casos, por personas que comparten características faciales similares. Otras aplicaciones como FaceLock, Luxand Face Recognition y True Key también presentan debilidades significativas en sus sistemas de reconocimiento facial.

En cuanto a las huellas dactilares, estas pueden ser objeto de suplantación de identidad y ataques de repetición. El reconocimiento de voz, por su parte, puede verse afectado por variaciones en los patrones vocales, mientras que el escaneo de iris puede presentar problemas cuando se utilizan gafas. Además, factores ambientales, como la iluminación y las condiciones de captura, pueden influir en la precisión de los diversos métodos biométricos.

Aunque los métodos biométricos se consideran generalmente más seguros que las técnicas tradicionales de autenticación, como las contraseñas, ninguno es completamente infalible. Estas tecnologías presentan vulnerabilidades en diferentes formas, como el spoofing, donde un atacante puede engañar al sistema utilizando huellas dactilares falsas o fotografías. Asimismo, los datos biométricos pueden ser interceptados durante su transmisión o almacenamiento, lo que compromete la seguridad del usuario. También existen riesgos de ataques de fuerza bruta y problemas relacionados con la privacidad, dado que, a diferencia de las contraseñas, los datos biométricos no pueden ser modificados una vez que han sido comprometidos.

La autenticación biométrica en aplicaciones móviles es un campo en constante evolución que busca mejorar la seguridad y experiencia de usuario. Las áreas de investigación futura en este campo son diversas. Los investigadores están explorando la integración de

múltiples modalidades biométricas, como el reconocimiento facial, la autenticación por voz y la verificación de firmas manuscritas, para crear sistemas más robustos y adaptables. Se está poniendo énfasis en el desarrollo de algoritmos más avanzados, utilizando técnicas de aprendizaje profundo y redes neuronales para mejorar la precisión y eficiencia. Además, se está investigando la integración de tecnologías emergentes como blockchain para aumentar la seguridad. La usabilidad y la experiencia del usuario son aspectos cruciales que están siendo estudiados, junto con la necesidad de realizar pruebas en entornos reales y con muestras más grandes de usuarios. La privacidad y la protección de datos biométricos son preocupaciones importantes, al igual que la interoperabilidad entre diferentes aplicaciones y plataformas. Los investigadores también están considerando los desafíos específicos de diferentes sectores, como la atención médica y las finanzas, y cómo la autenticación biométrica que puede adaptarse.

Conclusiones

En conclusión, esta revisión sistemática de la literatura sobre métodos de autenticación biométrica en aplicaciones móviles, basada en el análisis de 50 artículos, ha permitido identificar las principales modalidades utilizadas, como el reconocimiento facial, de voz y de huellas dactilares. Los hallazgos revelan que la autenticación biométrica ha ganado considerable popularidad, especialmente en el sector financiero, debido a su mayor nivel de seguridad en comparación con los métodos tradicionales.

Sin embargo, se han detectado vulnerabilidades, como los ataques de suplantación y problemas de precisión relacionados con factores ambientales. Mirando hacia el futuro, la investigación en autenticación biométrica para aplicaciones móviles se enfoca en mejorar la seguridad, usabilidad y adaptabilidad de los sistemas. Las áreas de investigación futura se centrarán en la integración de múltiples modalidades biométricas, el desarrollo de algoritmos avanzados y la adaptación a diversos contextos de uso, buscando un equilibrio entre seguridad y experiencia del usuario.

Referencias bibliográficas

Abazi, B., Qeliaja, B., & Hajrizi, E. (2019). Application of biometric models of authentication in mobile equipment. *IFAC-PapersOnLine*, *52*(25), 543–546. https://doi.org/10.1016/J.IFACOL.2019.12.602

Al Rousan, M., & Intrigila, B. (2020). A Comparative Analysis of Biometrics Types: Literature Review. *Journal of Computer Science*, *16*(12), 1778–1788. https://doi.org/10.3844/JCSSP.2020.1778.1788

Albalawi, S., Alshahrani, L., Albalawi, N., Kilabi, R., & Alhakamy, A. (2022). A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques. *International Journal of Advanced Computer Science and Applications*, *13*(4), 782–791. https://doi.org/10.14569/IJACSA.2022.0130491

Algarni, M. (2023). An Extra Security Measurement for Android Mobile Applications Using the Fingerprint Authentication Methodology. *Journal of Information Security and Cybercrimes Research*, *6*(2), 139–149. https://doi.org/10.26735/EPZF6556

Ali, G., Dida, M. A., & Sam, A. E. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet 2020, Vol. 12, Page 160*, *12*(10), 160. https://doi.org/10.3390/FI12100160

Ali, G., Dida, M. A., & Sam, A. E. (2021). A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications. *Future Internet 2021, Vol. 13, Page 299*, *13*(12), 299. https://doi.org/10.3390/FI13120299

Alwahaishi, S., & Zdralek, J. (2020). Biometric Authentication Security: An Overview. *Proceedings - 2020 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2020*, 87–91. https://doi.org/10.1109/CCEM50674.2020.00027

Ananthio, C., Andhini, T. M. W., Bakti, D. W., & Moniaga, J. V. (2023). Feasibility Study for Implementation Biometrics for Online Transaction. *Procedia Computer Science*, *227*. https://doi.org/10.1016/j.procs.2023.10.622

Anbalagan, N., Abbas Helmi, R. A., Hameed Ashour, M. A., & Jamal, A. (2020). Trusted Application Using Biometrics for Android Environment. *Proceedings - 2020 16th IEEE International Colloquium on Signal Processing and Its Applications, CSPA 2020*, 7–12. https://doi.org/10.1109/CSPA48992.2020.9068715

Ayeswarya, S., & Singh, K. J. (2024). A Comprehensive Review on Secure Biometric-Based Continuous Authentication and User Profiling. *IEEE Access*, *12*, 82996–83021. https://doi.org/10.1109/ACCESS.2024.3411783

Barlas, Y., Basar, O. E., Akan, Y., Isbilen, M., Alptekin, G. I., & Incel, O. D. (2020). DAKOTA: Continuous authentication with behavioral biometrics in a mobile banking application. *5th International Conference on Computer Science and Engineering, UBMK 2020*, 298–303. https://doi.org/10.1109/UBMK50275.2020.9219365

Basar, O. E., Alptekin, G., Volaka, H. C., Isbilen, M., & Incel, O. D. (2019). Resource Usage

Analysis of a Mobile Banking Application using Sensor-and-Touchscreen-Based Continuous Authentication. *Procedia Computer Science*, *155*, 185–192. https://doi.org/10.1016/J.PROCS.2019.08.028

Blanco-Gonzalo, R., Miguel-Hurtado, O., Lunerti, C., Guest, R. M., Corsetti, B., Ellavarason, E., & Sanchez-Reillo, R. (2019). Biometric Systems Interaction Assessment: The State of the Art. *IEEE Transactions on Human-Machine Systems*, *49*(5), 397–410. https://doi.org/10.1109/THMS.2019.2913672

Chandran, D. R., & Chandran, D. R. (2022). Use of AI Voice Authentication Technology Instead of Traditional Keypads in Security Devices. *Journal of Computer and Communications*, *10*(6), 11–21. https://doi.org/10.4236/JCC.2022.106002

Dijmarescu, I., Iatagan, M., Hurloiu, I., Geamanu, M., Rusescu, C., & Dijmarescu, A. (2022). Neuromanagement decision making in facial recognition biometric authentication as a mobile payment technology in retail, restaurant, and hotel business models. *Oeconomia Copernicana*, *13*(1), 225–250. https://doi.org/10.24136/OC.2022.007

Estrela, P. M. A. B., Albuquerque, R. de O., Amaral, D. M., Giozza, W. F., & de Sousa Júnior, R. T. (2021). A Framework for Continuous Authentication Based on Touch Dynamics Biometrics for Mobile Banking Applications. *Sensors 2021, Vol. 21, Page 4212*, *21*(12), 4212. https://doi.org/10.3390/S21124212

Estrela, P. M. A. B., De Oliveira Albuquerque, R., Amaral, D. M. E., Giozza, W. F., Nze, G. D. A., & De Mendonca, F. L. L. (2020). Biotouch: A framework based on behavioral biometrics and location for continuous authentication on mobile banking applications. *Iberian Conference on Information Systems and Technologies, CISTI*, *2020-June*. https://doi.org/10.23919/CISTI49556.2020.9140948

Fakhiroh, L. A., Fariza, A., & Basofi, A. (2021). Mobile Based Offline Handwritten Signature Forgery Identification using Convolutional Neural Network. *International Electronics Symposium 2021: Wireless Technologies and Intelligent Systems for Better Human Lives, IES 2021 - Proceedings*, 423–429. https://doi.org/10.1109/IES53407.2021.9594019

Galterio, M. G., Shavit, S. A., & Hayajneh, T. (2018). A Review of Facial Biometrics Security for Smart Devices. *Computers 2018, Vol. 7, Page 37*, *7*(3), 37. https://doi.org/10.3390/COMPUTERS7030037

Guidelines for performing Systematic Literature Reviews in Software Engineering. (2007).

Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An Improved Time-Based One Time Password Authentication Framework for Electronic Payments. *International Journal of Advanced Computer Science and Applications*, *11*(11), 359–366. https://doi.org/10.14569/IJACSA.2020.0111146

Incel, O. D., Gunay, S., Akan, Y., Barlas, Y., Basar, O. E., Alptekin, G. I., & Isbilen, M. (2021). DAKOTA: Sensor and Touch Screen-Based Continuous Authentication on a Mobile Banking Application. *IEEE Access*, *9*, 38943–38960. https://doi.org/10.1109/ACCESS.2021.3063424

Islam, I., Munim, K. M., Islam, M. N., & Karim, M. M. (2019). A proposed secure mobile money transfer system for SME in Bangladesh: An industry 4.0 perspective. *2019 International Conference on Sustainable Technologies for Industry 4.0, STI 2019*. https://doi.org/10.1109/STI47673.2019.9068075

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

Jeon, B., Jeong, B., Jee, S., Huang, Y., Kim, Y., Park, G. H., Kim, J., Wufuer, M., Jin, X., Kim, S. W., & Choi, T. H. (2019). A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation. *JMIR MHealth and UHealth*, *7*(4). https://doi.org/10.2196/11472

Karakaya, N., Alptekin, G. I., & İncel, Ö. D. (2019). Using behavioral biometric sensors of mobile phones for user authentication. *Procedia Computer Science*, *159*, 475–484. https://doi.org/10.1016/J.PROCS.2019.09.202

Khan, H. U., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2023). Role of authentication factors in Fin-tech mobile transaction security. *Journal of Big Data*, *10*(1), 1–37. https://doi.org/10.1186/S40537-023-00807-3/FIGURES/4

Kovalan, K., Omar, S. Z., Tang, L., Bolong, J., Abdullah, R., Ghazali, A. H. A., & Pitchan, M. A. (2021). A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users. *International Journal of Advanced Computer Science and Applications*, *12*(7), 829–837. https://doi.org/10.14569/IJACSA.2021.0120792

Kumari, K. (2024). Improving Payment Security with Deep Learning-Based Facial Recognition Systems in Mobile Banking Applications. *Journal of Sustainable Technologies and Infrastructure Planning*, *8*(3), 13–20. https://publications.dlpress.org/index.php/JSTIP/article/view/94

Liébana-Cabanillas, F., Kalinic, Z., Muñoz-Leiva, F., & Higueras-Castillo, E. (2024). Biometric m-payment systems: A multi-analytical approach to determining use intention. *Information & Management*, *61*(2), 103907. https://doi.org/10.1016/J.IM.2023.103907

Machap Marco, K. (2023). Facial Recognition Authentication Adds an Extra Layer of Security to Mobile Banking Systems. *Journal of Applied Technology and Innovation*, *7*(1), 2600–7304.

Medvedev, I., Shadmand, F., Cruz, L., & Gonçalves, N. (2021). Towards Facial Biometrics for ID Document Validation in Mobile Devices. *Applied Sciences 2021, Vol. 11, Page 6134*, *11*(13), 6134. https://doi.org/10.3390/APP11136134

Morake, A., Khoza, L. T., & Bokaba, T. (2021). Biometric technology in banking institutions: “The customers” perspectives’. *South African Journal of Information Management*, *23*(1), 1–12. https://doi.org/10.4102/SAJIM.V23I1.1407

Oduguwa, T., & Arabo, A. (2024). Passwordless Authentication Using a Combination of

Cryptography, Steganography, and Biometrics. *Journal of Cybersecurity and Privacy 2024, Vol. 4, Pages 278-297*, *4*(2), 278–297. https://doi.org/10.3390/JCP4020014

Othman, M. A., Husin, H. S., & Ismail, S. (2024). MySIMS: A Hybrid Application of Face Recognition Attendance and Tuition Management System. *Proceedings of the 2024 18th International Conference on Ubiquitous Information Management and Communication, IMCOM 2024*. https://doi.org/10.1109/IMCOM60618.2024.10418293

Piotrowska, A. (2024). Determinants of consumer adoption ofbiometric technologies in mobile financialapplications. *Economics and Business Review*, *10*(1), 81–100.

Priesnitz, J., Huesmann, R., Rathgeb, C., Buchmann, N., & Busch, C. (2022). Mobile Contactless Fingerprint Recognition: Implementation, Performance and Usability Aspects. *Sensors 2022, Vol. 22, Page 792*, *22*(3), 792. https://doi.org/10.3390/S22030792

Prihodova, K., & Hub, M. (2020). Hand-Based Biometric Recognition Technique - Survey. *Advances in Science, Technology and Engineering Systems*, *5*(6), 689–698. https://doi.org/10.25046/AJ050683

Rivero Albarrán, D., Guerra Torrealba, L. R., Luis Fernando, Rivero Albarrán, D., Guerra Torrealba, L. R., & Luis Fernando. (2023). Seguridad y componentes nativos en una aplicación híbrida. *Revista Científica UISRAEL*, *10*(1), 131–150. https://doi.org/10.35290/RCUI.V10N1.2023.748

Roszczewska, K., & Niewiadomska-Szynkiewicz, E. (2024). Online Signature Biometrics for Mobile Devices. *Sensors 2024, Vol. 24, Page 3524*, *24*(11), 3524. https://doi.org/10.3390/S24113524

Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. *IEEE Access*, *9*, 34541–34557. https://doi.org/10.1109/ACCESS.2021.3061589

Salihbašic, A., & Orehovacki, T. (2019). Development of android application for gender, age and face recognition using OpenCV. *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019 - Proceedings*, 1635–1640. https://doi.org/10.23919/MIPRO.2019.8756700

Samet, S., Ishraque, M. T., Ghadamyari, M., Kakadiya, K., Mistry, Y., & Nakkabi, Y. (2019). TouchMetric: a machine learning based continuous authentication feature testing mobile application. *International Journal of Information Technology (Singapore)*, *11*(4), 625–631. https://doi.org/10.1007/S41870-019-00306-W/METRICS

Sharma, Y., Gupta, H., & Khatri, S. K. (2019). An Authentication Model for Online Transactions Using Biometric Security. *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, 7–11. https://doi.org/10.1109/ISCON47742.2019.9036284

Shuhidan, S. M., Hamidi, S. R., Syazwani, I., Hammood, W. A., Abdullah, R., Hammood, O. A., Banga, L., & Pillai, S. (2021). Impact of Behavioural Biometrics on Mobile Banking System.

Journal of Physics: Conference Series, *1964*(6), 062109. https://doi.org/10.1088/1742-6596/1964/6/062109

Sunaryono, D., Siswantoro, J., & Anggoro, R. (2021). An android based course attendance system using face recognition. *Journal of King Saud University - Computer and Information Sciences*, *33*(3), 304–312. https://doi.org/10.1016/J.JKSUCI.2019.01.006

Wang, X., Chen, Y., Yang, R., Shi, S., & Lau, W. C. (2020). *Fingerprint-Jacking: Practical Fingerprint Authorization Hijacking in Android Apps*.

Ximenes, A. M., Sukaridhoto, S., Sudarsono, A., Ulil Albaab, M. R., Basri, H., Hidayat Yani, M. A., Chang Choon, C., & Islam, E. (2019). Implementation QR Code Biometric Authentication for Online Payment. *IES 2019 - International Electronics Symposium: The Role of Techno-Intelligence in Creating an Open Energy System Towards Energy Democracy, Proceedings*, 676–682. https://doi.org/10.1109/ELECSYM.2019.8901575

Yang, Y., Guo, B., Wang, Z., Li, M., Yu, Z., & Zhou, X. (2019). BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. *Ad Hoc Networks*, *84*, 9–18. https://doi.org/10.1016/J.ADHOC.2018.09.015

Yildirim, N., & Varol, A. (2019). A research on security vulnerabilities in online and mobile banking systems. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*. https://doi.org/10.1109/ISDFS.2019.8757495

Zhang, X., Cheng, D., Jia, P., Dai, Y., & Xu, X. (2020). An Efficient Android-Based Multimodal Biometric Authentication System with Face and Voice. *IEEE Access*, *8*, 102757–102772. https://doi.org/10.1109/ACCESS.2020.2999115