المجلة السياسية والدولية

اسم المقال: الحوكمة الرقمية: التسجيل البابومتري وتحديات الخصوصية
اسم الكاتب: أ.م.د. علي دريول محمد الجبوري
رابط ثابت: https://political-encyclopedia.org/library/9916
تاريخ الاسترداد: 2026/11/22 18:26 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من الصفحة الخاصة بالمجلة السياسية والدولية على موقع المجلات الأكاديمية العلمية العراقية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

الحوكمة الرقمية: التسجيل البايومتري وتحديات الخصوصية

أ.م.د على دريول محمد الجبوري
جامعة بغداد / كلية العلوم السياسية
ali.dar@copolicy.uobaghdad.edu.iq

الملخص:

ان (Biometrics) البصمة البيو مترية تشير إلى استخدام الخصائص البيولوجية الفريدة للفرد، مثل بصمات الأصابع، والوجه، وقزحية العين، أو حتى الصوت، لتحديد الهوية،. لذلك هدف البحث إلى استعراض أبرز التقنيات المعاصرة بمجال توظيف الذكاء الاصطناعي في مجال التحقق البيو متري وتوفر (Biometrics) القياسات الحيوية وسيلة قوية وفعالة لتعزيز الأمن السيبراني للدول . اذ توفر (Biometric verification) المصادقة الحيوية أمانًا محسّنًا لقاعدة البيانات الحكومية وتجربة تقنية متطورة لكافة المستخدمين لها . اتبعت الدراسة المنهج التحليلي الذي يتضمن توضيحاً لأبرز التحديات التقنية المرافقة لتوظيف تقنيات الذكاء الاصطناعي بمجال تنفيذ (Biometric security) الأمان البيو متري والتحقق البيو متري. أظهرت النتائج انه يتطلب تنفيذ (Biometric security) الأمان البيو متري دراسة متأنية للطرق المناسبة، وضمان أمان البيانات، والتكامل مع (Two-factor authentication for biometric verification) المصادقة الثنائية للتحقق البيو متري، وصيانة الأنظمة بانتظام ، وفي التقييم العام، أظهرت النتائج أيضا أن أجهزة التعرف على الوجه مطلوبة بشدة وموصى بها من قبل كافة المديريات العامة لمكافحة المخدرات وشرطة الحدود للعديد من الدول العربية ومنها العراق ، لاستخدامها للسيطرة على المنافذ الحدودية.وفي الختام تكافح دول العالم المتقدمة منها والنامية الى اعتماد الحوكمة الرقمية وتنويع الاقتصاد الرقمي ويتمثل أحد المكونات الرئيسية لهذا التغيير في التركيز على الهوية الرقمية والتكنولوجيا البيو مترية، والتي تعد بالغة الأهمية لتحديث الخدمات الحكومية وتعزيز الأمن الوطني والقومي .

السمات الفسيولوجية والسلوكية الفريدة

الكلمات المفتاحية: الأمان البيومتري ، البصمة البيو مترية ، الخصائص البيولوجية ، الحوكمة الرقمية ، الذكاء الاصطناعي ، الامن السيبراني.

تاريخ الاستلام : ٢٠٢٥/٢/٩	تاريخ القبول: ٢٠٢٥/٤/٢٣	تاريخ النشر: ٢٠٢٥/٦/١

Digital Governance: Biometric Registration and Privacy Challenges

Assist. Prof. Dr Ali Daryoul Mohammed Al-Jubouri (PhD)
University of Baghdad / College of Political Science
ali.dar@copolicy.uobaghdad.edu.iq

Abstract

Objectives: Biometrics refers to the use of an individual's unique biological characteristics, such as fingerprints, face, iris, or even voice, to identify an individual. Therefore, the study aims to review the most prominent contemporary technologies in the field of employing artificial intelligence in the field of biometric verification. Biometrics provides a powerful and effective means to enhance cybersecurity for countries by taking advantage of unique physiological and behavioral characteristics. Biometric verification provides enhanced security for the government database and an advanced technical experience for all its users.

Methodology: The study follows the analytical approach that includes an explanation of the most prominent technical challenges associated with employing artificial intelligence technologies in the field of implementing (Biometric security) biometric security and biometric verification.

Results: The results shows that implementing (Biometric security) biometric security requires careful study of appropriate methods, ensuring data security, integration with (Two-factor authentication for biometric verification), and regular system maintenance. In the overall evaluation, the results also shows that identification devices face recognition is highly demanded and recommended by the General Directorate of Narcotics Control

Keywords: Biometric security, biometric fingerprint, biological characteristics, digital governance, artificial intelligence.

Receipt: 9/2/2024	Acceptance: 23/4/2025	Publication: 1/6/2025

المقدمة:

لقد كانت التكنولوجيا ولا تزال ركيزة أساسية للتنافسية والنمو بالنسبة للحكومات في جميع أنحاء العالم. فالدول القادرة على تسخير قوة التكنولوجيا، وخاصة التقنيات الجديدة والناشئة مثل الحوسبة السحابية والذكاء الاصطناعي، قادرة على زيادة الإنتاجية، وتعزيز الابتكار، وتحقيق وفورات في التكاليف، كل ذلك

مع التعامل بشكل أفضل مع مواطنيها ودعمهم. وقد أثبتت المنظمات التجارية بالفعل أهمية مواكبة أحدث الاتجاهات، والحكومات الآن تحذو حذوها لضمان عدم تخلف دولها عن الركب في العصر الرقمي.

وفي عالم رقمي متسارع التقدم التكنولوجي بتقنيات الذكاء الاصطناعي، تبرز الحاجة إلى عدة أمور منها اتباع أساليب دقيقة وآمنة للتحقق من الهوية وضمان الأمان الرقمي للمواطنة الرقمية، وواحدة من أبرز هذه الأساليب التقنية المتطورة هي البصمة البيو مترية، التي تعتمد على الخصائص الحيوية الفريدة لكل فرد مثل بصمات الأصابع، نمط الوجه، وقزحية العين، وضرورة خضوع مستقبل عمل الجهاز الحكومي في جميع أنحاء العالم الى العالم الرقمي والمراجعة المستمرة بل والى الكثير من النقاشات والنقد بغية استشراف طبيعة ودور الحكومات في تطويرً القطاعات الحيوية المختلفة فضلا عن دورها في تطوير الخدمات المقدمة لمواطنيها ورفاهية مجتمعاتها، وفي أي سياق للحوكمة الرقمية، تأتي التكنولوجيا في المقام الأول والابرز فالعنصرين الرئيسيين اللذان يتحكمان بمستوى التقدم والنجاح في مبادرات الحوكمة الرقمية معتمدان على عنصران :

الأول: الاستخدام والتمثيل الأمثل لتكنولوجيا المعلومات والذكاء الاصطناعي.

الثاني: مدى قدرة الحكومات على انشاء القيمة المضافة منها لتطوير بنيتها التقنية الرقمية البيو مترية .

فالحوكمة الرقمية التي ترتكز في أساسها على محورية المواطن(Centric-Citizen Government).وتهدف إلى تمكين المواطن من الوصول إلى جميع أشكال وخدمات الحوكمة الرقمية، على المستوى المحلي او الدولي، وفي هذا السياق، يزداد الطلب وعلى نحو مطرد في جميع أنحاء العالم، علىً ضرورة تحول الحكومات من وظيفتها التقليدية في كونها نموذج القيام بمهام إدارية محددة(centric-Department) ، إلى نموذج مرتكز علىّ الوصول إلى الخدمات الرقمية او الحوكمة الرقمية والتواصل معُ متطلبات الجمهور، والتعامل مع وحداته ومؤسساته الإدارية الرسمية في ظل الحوكمة الرقمية والبصمة البيو مترية كأحدث واهم تطبيقاتها ، وهذه التقنية ليست مجرد خطوة نحو مستقبل رقمي أكثر أمانًا وفعالية، بل هي أيضًا تثير الكثير من النقاش حول حماية الخصوصية والمخاطر المحتملة وتتعدد تطبيقات البصمة البيو مترية في مختلف المجالات منها ما يخص الامن الوطني ، اذ تستخدم الدول البصمة البيو مترية والتحقق البيو متري في تتبع المشتبه بهم والتحقق من هويتهم في المعابر الحدودية وفي مجال الخدمات المصرفية والقطاع الصحي وأخيرا في التكنولوجيا الشخصية مثل الهواتف الذكية وأجهزة الكمبيوتر المحمولة اذ تستخدم تقنية البصمة البيو مترية كوسيلة لفتح الأجهزة والوصول الى المعلومات الشخصية فالحكومة الهندية أنشأت قاعدة بيانات بيو مترية تتضمن بصمات أصابع وعيون كل المواطنين في إطار مشروع يدعى "أدهار"، وفي سنة ٢٠٠٩ أطلقت نظام (أدهار) للتثبت من الهويات بشكل رقمي لمكافحة الفساد

في الإدارة والغش في نظام الضمان الاجتماعي، وعلى ضوء هذه المعطيات يبدو أن التمتع بحق المواطنة الرقمية بات حكرا على الأشخاص الذين يملكون بيانات بيو مترية.

فهل يمكن ان يصبح وجه الانسان بمثابة جواز سفر او تذكرة طائرة مستقبلا؟ أن الأمر قد يصبح واقعا في حال اعتمدت الولايات المتحدة الاريكية والاتحاد الاوربي والصين وبقية دول العالم على التقنيات البيو مترية، فالحكومة الأسترالية مثلا ترغب في إطلاق نظام أطلقت عليه اسم "وورلد فيرست" سنة ٢٠٢٠ تمت تطبيقه ٢٠٢٥يتيح للمسافرين إمكانية السفر دون الحاجة لإظهار وثائقهم من خلال التعرف على خصائصهم البيو مترية على غرار بصمات الأصابع والعين وتقنية البصمة البو مترية تعتبر من التقنيات الرائدة في مجال الأمن الرقمي والتحقق من الهوية في الدول العربية، وقد بدأت تطبيقاتها تتوسع في مجالات مختلفة مثل

الهواتف الذكية، أجهزة الكمبيوتر، البنوك، المؤسسات الحكومية، والمطارات الخ ويعود سبب ذلك الى عدة مزايا توفرها البصمة البيو مترية ومنها:

١. البصمات البيو مترية تقدم مستوى عال من الدقة في التحقق من الهوية مما يقلل من احتمال الاحتيال او التزوير او الخطأ.
٢. ان تقنية البيو مترية سهلة وسريعة التحقق من الهوية دون الحاجة الى حمل بطاقات او تذكر كلمات مرور.
٣. تحسين الأمان وكفاءة العمليات لأنه باستخدام الخصائص الفريدة لكل فرد يمكن تعزيز الأمان في الأماكن التي تتطلب مستويات عالية من الحماية مثل المطارات والبنوك وكذلك تقليل الوقت والجهد المبذول في التحقق من الهوية والمحصلة النهائية المساهمة في تحسين الكفاءة في العديد من العمليات اليومية .

لذلك تستند المنصة البيو مترية في اية دولة تستخدمها إلى ' نواة بيومترية'وتشمل قاعدتي بيانات الإنتربول الدولية المخصصتين لبصمات الأصابع وتحديد سمات الوجه ومنظومة مقارنة تقوم على تقنية ((IDEMIA))، وهذه المنصة التي أُطلقت في تشرين الأول/أكتوبر ٢٠٢٣ ستوضع تدريجيا، خلال سنتين، بتصرف المراكز الحدودية وأفراد الشرطة في الخطوط الأمامية في بلدان الإنتربول الأعضاء، ويتوقَّع أن تعامل هذه المنظومة يوميا مليون تقصّ انطلاقا من بيانات أدلة جنائية من قبيل بصمات الأصابع وبصمات الراحات وصور الوجه، وهذه الأداة الفعالة المخصصة للتدقيق في الأشخاص على الحدود يمكن أن تُستخدَم أيضا لعمليات الشرطة الاعتيادية التي تنفَّذ في أحد البلدان للتحقق مما إذا كان شخص ما يخضع للتدقيق يطرح تهديدا أمنيا، وهذا عامل بالغ الأهمية عندما لا تتوفر وثائق سفر وقال السيد سيريل غو : مدير الدعم العملياتي والتحليل في الإنتربول، ويمكن لأحد الجناة الفارّين تغيير اسمه

وجوانب عديدة من مظهره من أجل الفرار من وجه العدالة، ولكن من الصعب لا بل من المستحيل تغيير البيانات البيو مترية ، لذا تبقى هذه البيانات أوثق الوسائل لتحديد هوية شخص ما مثلا ، بعد إطلاق المنصة الجديدة بوقت قصير، أفضت عملية للإنتربول إلى اعتقال مهرّب مهاجرين فارّ وكان في حوزة المذكور جواز سفر مزور أثناء تدقيق شرطي وطني أُجري في سراييفو (البوسنة والهرسك)، وعندما أُدخلت صورته في المنصة البيو مترية تبين أنها تطابق صورة شخص مطلوب في بلد آخر لتهريب مهاجرين وجريمة منظمة وتشمل البيانات البيو مترية مجموعة متنوعة من التقنيات المختلفة التي تستخدم المطابقة الاحتمالية للتعرف على شخص ما بناءً على خصائصه الحيوية. يمكن أن تكون الخصائص الحيوية عبارة عن سمات فسيولوجية (على سبيل المثال، بصمة إصبع الشخص، أو قزحية العين، أو هندسة الوجه أو اليد)، أو سمات سلوكية (مثل مشية الشخص، أو توقيعه، أو نمط ضغط المفاتيح).

ونظرًا لأن الخصائص البيو مترية فريدة من نوعها بشكل عام للأفراد، فقد تكون أكثر فعالية وموثوقية في التحقق من هويات الأفراد بشكل فريد من الطرق الأخرى مثل أنظمة التحقق القائمة على المعرفة (على سبيل المثال، كلمة المرور أو رقم التعريف الشخصي) أو الأنظمة القائمة على الرموز (على سبيل المثال، بطاقة الهوية أو الترخيص) ومن المزايا الأخرى أن الخصائص البيو مترية لا يمكن مشاركتها أو فقدها أو تكرارها بسهولة مثل كلمات المرور أو الرموز. وعلى هذا النحو، تُستخدم البيانات الحيوية بشكل متزايد في إدارة الهوية، وخاصة لأغراض المصادقة (أي التأكد من أن الشخص هو من يدعي أنه هو).

وعندما تُدخَل صورة وجه في المنظومة (صورة للمقارنة)، فإنها ترمَّز تلقائيا بواسطة خوارزمية وتقارَن مع ملفات الصورة المسجلة في المنظومة. والنتائج هي قائمة صور مرشحة لأكثر المطابقات احتمالا وواحيانا جهات انفاذ القانون تستخدم او تنفذ على الدوام عملية يدوية – يسميها المختصين بالبصمة البيو مترية تحديد الهوية من خلال التعرف على سمات الوجه – للتحقق من النتائج التي توصلت إليها المنظومة الآلية. ثم يقوم موظفون مؤهلون وذوو خبرة من الإنتربول بمقارنة الصور بعناية للعثور على خصائص فريدة يمكن أن تؤدي إلى "صورة مرشحة محتملة" أو "لا صور مرشحة" أو إلى نتيجة "غير حاسمة ، وتحال هذه المعلومات إلى البلدان التي زودت بالصور، أو التي قد تكون معنية بالسمات أو بمطابقة. ثم تُعامَل الإشعارات بما ينسجم ونظام الإنتربول لمعاملة البيانات الذي يضمن قانونية وجودة المعلومات وحماية البيانات الشخصية وإن جميع صور الوجوه في النشرات والتعاميم التي تطلب البلدان الأعضاء إصدارها يتم تقصّيها وتُخزن في منظومة تحديد سمات الوجه، شريطة أن تستوفي معايير الجودة الصارمة اللازمة لتحديد سمات الوجه.

ويمكن للبلدان الأعضاء أيضا أن تطلب إجراء تقصّ من نوع "البحث فقط" في المنظومة، وذلك على سبيل المثال للأشخاص ذوي الأهمية الخاصة في المطارات أو المعابر الحدودية الأخرى. وتصدر النتائج

بسرعة لتيسير اتخاذ إجراءات المتابعة بشكل فوري، ولا تُسجَّل الصور في المنظومة، وبما أن هذه التكنولوجيا لتحديد سمات الوجه بمساعدة الحاسوب ما فتئت في بداياتها في معظم البلدان، فإن المعايير وأفضل الممارسات لا تزال في طور الإنشاء، ويساهم الإنتربول في ذلك لما كانت منظومات تحديد سمات الوجه تنطوي على إمكانات هائلة في مجال السلامة والأمن الوطنيين، فإنها تتطلب بنية إدارية متينة من أجل حماية حقوق الإنسان والبيانات الشخصية.

أهمية البحث:

تنطلق أهمية البحث بتقديم نظرة عامة شاملة عن الحوكمة الرقمية وموقعها العالمي من خلال تحديد المؤشرات العالمية الرئيسية لها. ومن خلال تحليل هذه المؤشرات، نكتسب كباحثين نظرة ثاقبة للتقدم التكنولوجي الناجح في دول العالم حتى الآن ونسلط الضوء على المبادرات الرئيسية التي ساهمت في تقدمها. كما نتمكن من تحديد المجالات التي يجب مراعاتها للأولوية في المرحلة التالية من رحلتها التكنولوجية مع وضعها كقائدة في عصر الذكاء الاصطناعي.

ومن خلال هذا البحث نسعى إلى تقديم رؤى قيمة واستراتيجيات عملية وأفضل الممارسات التي ستمكن الحكومات العربية ومنها العراق من التعامل بفعالية مع تعقيدات التحول الرقمي. ومن خلال الاستفادة من خبرات وموارد شركات عالمية رائدة في مجال تكنولوجيا المعلومات والذكاء الاصطناعي لدعم تطلعات العراق ليصبح لاعباً رائداً في العصر الرقمي، وتعزيز الابتكار والكفاءة والخدمات التي تركز على خدمة المواطن العراقي.

وعليه تعتبر البصمة البيو مترية احدى اهم تطبيقات الحوكمة الرقمية بل ان البعض يعتبر ان استحداث المنصة البيو مترية والتحقق البيو متري سوف يسهم في مكافحة الإرهاب وحالات الاحتيال والتزوير الالكترونية لأنها (البصمة البيو مترية والتحقق البيو متري) عبارة عن منظومة متطورة جدا صُمِّمت لكشف المجرمين، وبفضل واجهتها السهلة الاستخدام، يمكن لأفراد إنفاذ القانون في كل دول العالم من خلال تحميل بصمات أصابع وصور للوجه تتولى برمجية متطورة بتقنية الذكاء الاصطناعي مقارنة شديدة الفعالية تقصّيها في البيانات المسجلة في قواعد بيانات الإنتربول الدولي البيو مترية بحثا عن مطابقات محتملة لكل الأشخاص المتهمين او المتورطين بأعمال إرهابية لذلك تكافح كافة الدول العربية ومنها العراق لتعزيز المكونات الرئيسية لهذه الرؤية المستقبلية بغرض تحقيق الاتي:

أولا: في التركيز على الهوية الرقمية والتكنولوجيا البيو مترية، والتي تعد بالغة الأهمية لتحديث الخدمات الحكومية وتعزيز الأمن الوطني ومنها نجاح مشروع بصمات الأصابع البيو مترية لكافة وزارات الداخلية العربية ومنها العراق وأن عملية أخذ البصمة البيو مترية تتم من خلال أخذ بصمة الوجه، وقزحية العين، بالإضافة إلى أخذ بصمات اليد والكف، وأخذ التوقيع الإلكتروني، لمن هم يتجاوزون (١٨) عاماً تلعب شركات مثل (STC) دورًا مهمًا في التقدم الرقمي وباعتبارها مشغل

اتصالات بارزًا، وسعت (STC) أبعد من الخدمات التقليدية لتلعب دورًا مهمًا في التحول الرقمي في دول الخليج العربي ، وتعمل هذه العقود على تحسين الاتصال في البلاد ومساعدة الحكومة في تحقيق أهدافها الرقمية الأوسع، مثل تمكين استخدام تكنولوجيا القياسات الحيوية. والذكاء الاصطناعي فإنها تساهم في تحقيق رؤية مستقبلية، وإعادة تشكيل مستقبل الدول العربية كانظمة متقدمة ومتطورة وعبر توظيف تكنولوجياً آمنة للحوكمة الرقمية.

ثانيا: تعتبر الدول العربية ومنها العراق ان الوصول إلى تقنيات الذكاء الاصطناعي وتوظيفها في مجال خدمات الحوكمة الرقمية حقًا عامًا وتلزم الجهات الحكومية بالعمل على ضمان الشمول الرقمي لكافة مؤسساتها الرسمية وتشمل العوامل التقنية الرقمية التي يجب أخذها في الاعتبار، على سبيل المثال لا الحصر، توفير البنى التحية اللازمة لأنشاء قاعدة حوكمة رقمية سهولة الوصول والاستخدام لكافة المستخدمين لها على مستوى مؤسسات الدولة والمواطنين والمقيمين والزائرين في هذه الدول.

ثالثا: نجحت دول الخليج العربي بتطبيق البصمة البيو مترية كأحد اهم منجزات الحوكمة الرقمية والمواطنة الرقمية والبصمة البيو مترية هي نوع من التقنيات الحيوية المستخدمة لتحديد الهوية والتحقق منها بناءً على الخصائص الفيزيولوجية والفسيولوجية الفريدة للأفراد.

اشكالية البحث:

في هذا البحث سنتناول مفهوم البصمة البيو مترية، فوائدها، وما هي الْمَخَاطِرِ الناجمة عن استخدامها، إلى جانب استعراض تطبيقاتها وتفاصيلها المختلفة. سنستكشف كيف يمكن لهذه التقنية أن تحسن حياة المواطن اليومية وما هي التحديات التي قد تواجه الدول العربية ومنها العراق في اعتمادها على نطاق واسع وذلك من خلال طرح التساؤلات الموضوعية الاتية:

وتأسيسا على ما تقدم، تتمثل اشكالية البحث في مناقشة اليات عمل البصمة البيو مترية وتحدياتها التقنية في دول العالم اذ يسعى البحث الى الإجابة عن الأسئلة الاتية:

- ماهي البصمة البيو مترية وكيف تعمل؟ وما هي الْمَخَاطِرِ؟
  - هل الاعتماد المفرط على التكنولوجيا البيو مترية يمكن ان يكون ضارا في حالة حدوث أخطاء تقنية او اعطال في النظام مما يعطل العمليات الحيوية للأفراد والشركات والمؤسسات في الدول العربية؟
  - هل يمكن استخدام البصمات البيو مترية بطريقة غير قانونية او قسرية؟ وهل يثير ذلك الاستخدام لتلك البيانات قضايا أخلاقية وقانونية؟
  - هل يمكن استخدام البيانات البيو مترية المسروقة في عمليات احتيال او انتحال شخصية؟
- ما أبرز تحديات تطبيق البيو مترية .

- وما إمكانية وضع تصور مقترح لمستقبل الحوكمة الرقمية والبصمة البيو مترية الدول العربية ومنها العراق؟

اهداف البحث:

يسعى البحث الى تحقيق هدفه الرئيس المتمثل في الأمور الاتية:

أولا: لقد أصبح التحول الرقمي ضرورة قصوى للحكومات في جميع أنحاء العالم وهي تتنقل بين تحديات هذا المشهد الديناميكي. وفي هذا العصر من التقدم التكنولوجي السريع، يجب على الحكومات تقييم نضجها الرقمي، وتصور المشهد الرقمي المستقبلي، وتطوير استراتيجيات شاملة للريادة في العصر الرقمي.

ويهدف هذا البحث إلى تقديم رؤى قيمة وتوصيات استراتيجية، مخصصة للكويت بناءً على تعاونها مع الشركات العالمية الرائدة في تكنولوجيا المعلومات والذكاء الاصطناعي ومنها شركة مايكروسوفت وغيرها وبصفتها شريكًا استراتيجيًا كدولة تمتلك مزايا القوة الاقتصادية المتميزة في منطقة الشرق الأوسط وغرب اسيا وتلتزم هذه الشركات العالمية الرائدة بتكنولوجيا المعلومات بدعم الحكومات العربية وبخاصة دول الخليج العربي لقيادة أجندة التحول الرقمي الخاصة بها كدولة قائدة في العصر الرقمي.

ثانيا : يهدف البحث الى التأكيد على البعد الأمني في تطبيق البصمة البيو مترية كاطار مفاهيمي وبخاصة في مكافحة الإرهاب وغسيل الأموال وتمويل الجماعات الإرهابية ، لأنه من خلال البصمة البيو مترية والتحقق البيو متري يمكن التعرف على المجرمين ومهما كانت تقنيات التخفي التي يستخدمونها فتحديد سمات الوجه بمساعدة الحاسوب هو تكنولوجيا حديثة العهد نسبيا، تستخدمها أجهزة إنفاذ القانون في العالم أجمع لتحديد أشخاص ذوي أهمية خاصة بالنسبة إليها على صور وجوه وردت من أكثر من (١٧٩) بلدا، الأمر الذي يجعلها قاعدة بيانات جنائية عالمية فريدة من نوعها ، وتحتوي منظومة الإنتربول لتحديد سمات الوجه ويمكن لهذه المنظومة، إذا استُخدمت بالاقتران ببرمجية بيومترية و مؤتمتة،(IFRS) تحديد هوية شخص أو التحقق منها من خلال مقارنة وتحليل أنماط سمات الوجه والملامح وأشكالها وأبعادها ، لقد جرى تحديد هوية ما يناهز (١٥٠٠)شخص من الإرهابيين والمجرمين والفارّين وذوي الأهمية الخاصة والمفقودين منذ إطلاق منظومة الإنتربول لتحديد سمات الوجه في نهاية عام ٢٠١٦ عوامل تحديد الهوية من خلال التعرف على سمات الوجه.

وبخلاف بصمات الأصابع والبصمة الوراثية، التي لا تتغير خلال حياة الشخص، يجب أن تأخذ برمجية تحديد سمات الوجه في الاعتبار عوامل مختلفة، مثل التقدم في السن، الجراحة التجميلية، مستحضرات التجميل، آثار تعاطي المخدرات أو التدخين، وضعية الشخص الصحية او سجله الصحي، والعمل استنادا إلى صور جيدة النوعية هو أيضا مسألة بالغة الأهمية. فالصور المنخفضة أو المتوسطة النوعية قد

يتعذر تقصّيها في منظومة IFRS وإذا أمكن تقصّيها فقد تؤثر هذه النوعية سلبا إلى حد بعيد في دقة البحث وفي النتائج نفسها، ولعل الصورة الشخصية الاعتيادية في جواز السفر المقبول من منظمة الطيران المدني الدولي (الإيكاو) هي خيار مثالي: فهي صورة أمامية للشخص المعني، مع إضاءة موحّدة تغطي كامل الوجه وخلفية محايدة

ثالثا : في مناقشة موضوعة تزايد وتوسع استخدام التقنيات والأنظمة البيو مترية بشكل كبير في القطاعين العام والخاص، اذ أصبحت التقنيات البيو مترية (على سبيل المثال التعرف على الوجه، أو الصوت، أو بصمات الأصابع أو تقنيات مسح القزحية) أرخص وأكثر تقدمًا ودقة، ونتيجة لذلك، أصبحت أكثر تكاملاً في الحياة اليومية للمواطن، وفي تفاعلاتهم مع الحكومة. وتتضمن هذه الخصائص السمات الفيزيائية مثل بصمات الأصابع، قزحية العين، نمط الوجه، ونمط الصوت. يتم جمع هذه البيانات الحيوية واستخدامها للتحقق من هوية الشخص بطريقة دقيقة وفعالة.

فرضية البحث:

يؤدي اعتماد أنظمة التسجيل البايومتري في إطار الحوكمة الرقمية إلى تعزيز كفاءة الخدمات الحكومية، إلا أنه في المقابل يُثير تحديات جوهرية تتعلق بخصوصية الأفراد وحماية بياناتهم الشخصية، نتيجة لغياب الأطر القانونية والتقنية الكافية لضمان الاستخدام الآمن والمسؤول لهذه البيانات.

منهجية البحث:

تكمن منهجية البحث في توظيف منهج التحليل النظمي، لغرض التغلغل في عمق الموضوع و تحليل كافة المعطيات و تفسير الظواهر و المتغيرات و تركيب العمليات المجتمعة و الظاهرة البحثية (إشكالية الدراسة) و دراسة أبعادها و تقويمها .

المبحث الأول

البايومترية (Biometrics) والخصائص الفسيولوجية أو السلوكية الفريدة للمواطنة الرقمية

مع تقدم التكنولوجيا، تتقدم أيضًا الأساليب التي يستخدمها مجرمو الإنترنت لاختراق أنظمة الأمان. أصبح من الضروري للدول تنفيذ تدابير أمنية سيبرانية قوية لحماية بياناتها الحساسة وضمان سلامة عملائها. أحد المكونات الرئيسية في هذه المعركة ضد التهديدات السيبرانية هو (Biometrics) ، والتي توفر طرقًا فريدة وآمنة للتحقق من هوية الأفراد. في هذه المقالة، سوف نستكشف دور القياسات الحيوية في الأمن السيبراني، والتهديدات التي تواجهها، والحلول المتاحة لمعالجة هذه التحديات. (Alan & Julia 2013)،(zreter 2007,67-86)،(Hosein &Martin 2010)

ما هي البايومترية (Biometrics) ؟

مصطلح القياسات الحيوية مشتق من الكلمتين اليونانيتين bios(حياة) و metrikos(قياس). القياسات الحيوية هي عبارة عن طرق آلية للتعرف على الفرد بناءً على خصائص بيولوجية وسلوكية قابلة للقياس. يتم التعرف من خلال قياس وتحليل الخصائص الفسيولوجية والسلوكية البشرية.

وتشير البصمة البيومترية إلى استخدام الخصائص الجسدية والسلوكية لتحديد الأفراد بشكل فريد. يمكن أن تشمل هذه الخصائص بصمات الأصابع، وملامح الوجه، وأنماط الصوت، ومسح القزحية/شبكية العين، وحتى إيقاع الكتابة، على عكس كلمات المرور أو الرموز، والتي يمكن فقدها أو سرقتها بسهولة، فإن القياسات الحيوية البصمة البيو مترية متأصلة في الأفراد، مما يجعل من الصعب تزويرها أو تكرارها. (Cyber Security Framework 2018) ، (Evrensel 2010) ، (Hosein & Nyst 2013)

Figure(١): Types of biometrics: some examples of physiological and behavioral measurements



وعلى الرغم تقدم الحكومة العديد من الخدمات، ولكن الوصول إلى الخدمات الحكومية في البلدان النامية مهمة صعبة للغاية. يقضي المواطنون هناك وقتًا طويلاً ويحتاجون إلى الخضوع لإجراءات طويلة للوصول إلى الخدمات الحكومية مثل خدمات جوازات السفر، وتبادل المعلومات، ودفع الفواتير، وملء الضرائب، والخدمات المصرفية وما إلى ذلك. والأنظمة بأكملها يدوية، لذا فهي بطيئة جدًا وتستغرق وقتًا طويلاً. ، (Tynan ٢٠١٣)

(Devereau & Vincent 2010, 367-379) ، (McDowell 2000)

لذا فهناك حاجة أساسية لتحقيق الكفاءة والشفافية والموثوقية في النظام الحكومي. يستخدم النظام الحكومي تكنولوجيا المعلومات لتقديم خدمات أفضل للمواطن، ويطلق على ذلك اسم الحوكمة الرقمية، وفي كل بلد، عندما تقدم الحكومة خدمات إلكترونية، من الضروري تحديد هوية المواطن لغرض الترخيص. في التشفير العام، يعتمد المصادقة على بيانات الاعتماد مثل كلمة المرور ومعرف المستخدم. ولكن هناك العديد من القيود في التعريف التقليدي أو اليدوي مثل صعوبة حفظها، وأغلب كلمات المرور سهلة التخمين مما يعرض الأمن للخطر؛ إن كلمات المرور المعقدة يصعب تذكرها، لذا يخزنها الناس في أماكن يسهل الوصول إليها. ويتمثل أحد الحلول لهذه المشكلة في تصميم معرف فريد لكل مواطن. على سبيل المثال، أنشأت حكومة الهند هيئة الهوية الفريدة بتكليف بإصدار هوية فريدة لجميع المقيمين في البلاد. وتقترح هيئة الهوية الفريدة إنشاء منصة لجمع التفاصيل البيو مترية أولاً ثم إجراء المصادقة التي يمكن استخدامها من قبل العديد من مقدمي الخدمات الحكومية والتجارية. (Liu 2009, 237-250) .

تُستخدم البيانات الحيوية عادةً للتحقق من هوية الشخص. ومن الأمثلة على ذلك التعرف على بصمات الأصابع أو الوجه للوصول إلى الهواتف الذكية، أو استخدام تقنية التعرف على الوجه في بوابات المطارات الذكية. يُعرف استخدام البيانات الحيوية لغرض التحقق من هوية الأفراد أيضًا باسم المطابقة من واحد إلى واحد.

في أنظمة المصادقة الحيوية من واحد إلى واحد (١:١)، تتم مقارنة الخصائص الحيوية للشخص بالبيانات الموجودة التي يحتفظ بها النظام بالفعل لهذا الفرد. في هذه الحالة، قدم الفرد معلوماته الحيوية مسبقًا لأغراض المصادقة المستقبلية. (Nabti & Bouridane 2008) .

تتطلب معظم أنظمة المصادقة الحيوية المستخدمة للمصادقة من الفرد تقديم خصائصه الحيوية بشكل نشط، والتي يتم مطابقتها بعد ذلك بالمعلومات الحيوية الموجودة في قاعدة البيانات. ومع ذلك، يمكن أن تحدث المصادقة بشكل سلبي أيضًا، حيث لا يتعين على الفرد القيام بدور نشط في العملية.

بدلاً من ذلك، يتم جمع خصائصه الحيوية والمصادقة عليها في الخلفية أثناء تعامل الفرد مع المنظمة أو الخدمة. على سبيل المثال، قد يتم جمع بيانات صوت الشخص والتحقق من صحتها أثناء حديثه إلى ممثل خدمة العملاء عبر الهاتف.(Poli& Arcot 2009 , 261-269)

تُستخدم البيانات الحيوية السلوكية بشكل متزايد للمصادقة السلبية، غالبًا كطبقة إضافية من الأمان. وكما ذكرنا أعلاه، يتضمن هذا قياس وتتبع الأنماط في الطريقة التي يتحرك بها الفرد أو يتصرف أو يستخدم شيئًا ماديًا. يمكن أن يتراوح هذا من كيفية حمل الشخص لجهاز وتحريكه، مثل الهاتف المحمول، إلى كيفية نقر أصابعه على الشاشة وقوة نقراته. حتى اللغة التي يستخدمها الشخص (على سبيل المثال، اختياره للكلمات والقواعد وبنية الجملة) يمكن قياسها كسمة حيوية Shaikh and Rabaiotti 2010, (63-204).

النوع الثاني من أنظمة القياسات الحيوية هو نظام واحد إلى اكثر (N:١) والذي يستخدم غالبًا لتحديد هوية الأفراد، ويتضمن ذلك مقارنة السمات الحيوية لشخص غير معروف بخصائص أخرى من نفس النوع في قاعدة البيانات (على سبيل المثال، بصمة الشخص مقابل بصمات أصابع أخرى في قاعدة البيانات).

(E-government Development Index (EDGI) 2022)

والهدف من أنظمة واحد إلى كثير هو إنتاج تطابق محتمل، وبالتالي تحديد هوية ذلك الشخص. ولا يتم ضمان التطابق دائمًا، حيث قد تكون المعلومات الحيوية لذلك الفرد المحدد موجودة أو لا تكون موجودة في قاعدة البيانات.

ومن الأمثلة على أنظمة القياسات الحيوية من واحد إلى كثير استخدام تقنية التعرف على الوجه لتحديد هوية شخص في حشد من الناس. وغالبًا ما تُستخدم أنظمة واحد إلى كثير أيضًا في سياق إنفاذ القانون، على سبيل المثال لمطابقة الحمض النووي الموجود في مسرح الجريمة مع عينات أخرى في قاعدة البيانات، من أجل تحديد هوية الضحية أو الجاني .(Shaikh & Rabaiotti 2010, 63-204) ، (Alrai 2011) ، (Roberts 2005)

ويمكن أن تعمل أنظمة القياسات الحيوية مع تقنيات أخرى لأغراض تتجاوز المصادقة أو التعريف. على سبيل المثال، بالإضافة إلى تحديد هوية الفرد، يمكن استخدام تقنية التعرف على الوجه لأغراض المراقبة أو الرصد – بمجرد تحديد هوية الشخص، يمكن تعقبه (على سبيل المثال، باستخدام شبكة من كاميرات المراقبة التلفزيونية المغلقة) أثناء تحركه في بيئة ما. عادة ما تكون الأنظمة البيو مترية آلية، وأحيانًا تستخدم الذكاء الاصطناعي لإجراء عملية التعرف. (Al-Raisi & Al-Khouri 2008, 117-132)

وتشير البصمة البيو مترية والتحقق البيو متري إلى المصادقة التلقائية على هوية شخص ما على أساس خصائصه الفسيولوجية أو السلوكية الفريدة والنظام البيو متري هو نظام التعرف على الأنماط الذي يعمل عن طريق الحصول على البيانات البيو مترية من شخص ما، واستخراج مجموعة من الميزات ومقارنتها بمجموعة القوالب المخزنة في قاعدة البيانات. اعتمادًا على السياق، قد تعمل الأنظمة البيو مترية إما في وضع التحقق أو وضع التعريف.

في وضع التحقق، يقوم النظام بمصادقة هوية الشخص عن طريق مقارنة البيانات البيو مترية التي تم الحصول عليها مع القوالب البيو مترية المخزنة في قاعدة بيانات النظام. التحقق هو التعرف الإيجابي؛ حيث يكون الهدف هو تجنب استخدام أشخاص متعددين لنفس الهوية. أثناء وضع التعريف، يميز النظام الفرد عن طريق البحث في قوالب جميع المستخدمين المخزنة في قاعدة البيانات عن تطابق. (Amoore 2006, 336– 351)

التعريف هو التعرف السلبي: منع شخص واحد من استخدام هويات متعددة. في حين أن التقنيات التقليدية للتعرف على الشخصية مثل كلمات المرور وأرقام التعريف الشخصية والرموز والمفاتيح قد تنجح في التعرف الإيجابي، فإن التعرف السلبي لا يمكن تحديده إلا من خلال البصمة البيو مترية.(Global Knowledge Index 2022).

المبحث الثاني

تقنيات عمل الأنظمة البيو مترية

يتم إدخال المعلومات البيو مترية للشخص في البداية في نظام بيو متري عند نقطة تُعرف باسم التسجيل. أثناء عملية التسجيل، يتم جمع سمة لتكون بمثابة معلومات مرجعية بيو مترية لذلك الشخص. يمكن تسجيل هذه المعلومات كبيانات خام (مثل صورة بصمة الإصبع) أو قالب رقمي. في القالب الرقمي، يتم استخراج السمات الرئيسية للسمة البيو مترية ومعالجتها لإنشاء القالب، والذي يتم تخزينه في قاعدة بيانات للاستخدام في المستقبل.

عند تقديم المعلومات البيو مترية في مرحلة لاحقة (غالبًا ما تُعرف باسم التعرف)، تحدث نفس العملية: يتم اكتشاف سمة الشخص، واستخراج السمات الرئيسية، ثم مطابقتها مع القوالب الموجودة في قاعدة البيانات، إما للمصادقة أو تحديد هوية ذلك الشخص .(Global Knowledge Index 2022) ، (Galbally & Alonso-Fernandaez 2012 , 311-321),(Hosein 2005, 594-625) .

وتخزن معظم الأنظمة البيو مترية القالب فقط، وليس صورة السمات البيو مترية المادية. ومع ذلك، في بعض الحالات، قد يتم الاحتفاظ بالصور الأصلية لخصائص التسجيل (على سبيل المثال، صور

بصمات الأصابع) أيضًا. يعتقد بعض المشغلين أن هذا ضروري في حالة الحاجة إلى إعادة التحقق لاحقًا، إلا أنه ينطوي على بعض المخاطر، كما سنرى لاحقًا في هذه الدراسة.
وإن القوالب التي يتم إنشاؤها وتخزينها تكون عادةً فريدة من نوعها لحل القياسات الحيوية هذا، وحتى في بعض الأحيان تكون فريدة من نوعها لنموذج محرك التعرف. لن يتم التعرف على القالب الذي تم إنشاؤه بواسطة محرك القياسات الحيوية الخاص بشركة مصنعة بواسطة نظام تم إنشاؤه بواسطة بائع آخر. في بعض الأحيان، لن يكون القالب الذي تم إنشاؤه بواسطة إصدار سابق من البرنامج من شركة مصنعة واحدة قابلاً للقراءة بواسطة إصدار لاحق. (Abdul Sattar, Aya Jaafar& Salih ,Yusra Mahd 2022)

وبناءً على ذلك، فإن تخزين القوالب يأتي بمخاطر أقل بكثير من تخزين الخصائص الحيوية الخام مثل صورة بصمة الإصبع. ومع ذلك، على الرغم من المخاطر المنخفضة قليلاً، يجب تشفير القوالب. وحيث يتم تخزين الصور الخام للقياسات الحيوية، فإن ضوابط الأمان ضرورية ويجب إجراء مراقبة وتدقيق منتظمين لهذه الضوابط. يجب على المنظمات أيضًا أن تفكر فيما إذا كانت ترغب في أن تصبح هدفًا للمجرمين الذين يسعون إلى الحصول على بيانات حيوية يمكن استخدامها لسرقة الهواتف(Lewela & Kisiangani 2013) ،
( ) ، Lewela & Kisiangani (Alwan 2022) ، (Abed kadhim& Ibrahim 2022) ٢٠١٣Namuq 2019)

وفيما يلي وصف للبصمة البيو مترية المستخدمة بشكل شائع:
أولا: التعرف على الوجه:الخاصية الحيوية الأكثر شيوعًا التي يستخدمها البشر للتعرف على الشخصية هي صورة الوجه. وتستخدم جميع الأنظمة الحيوية نفس المعلومات للتعرف على الوجه، وتستند أكثر الأساليب قبولًا إلى الاتي:
أ) موضع وشكل وحجم ملامح الوجه، مثل الحاجب والعينين والأنف والشفتين والذقن وارتباطها المكاني.
ب) التحليل الشامل لصورة الوجه والذي يمثل الوجه كمزيج من عدد من الكائنات (الأنماط).

ثانيا: بصمة الإصبع: بصمات الأصابع عبارة عن خطوط رسومية تشبه التدفق على أصابع الإنسان. تتميز الخطوط والأخاديد الجلدية الفردية بخصائص مختلفة لأصابع مختلفة. إن التكوين والتفاصيل الدقيقة للخطوط والأخاديد الفردية دائمة ولا تتغير بالنسبة لإصبع معين، لذا فإن بصمات الأصابع هي السمة الحيوية الفعالة.

ثالثا: القزحية: القزحية هي نوع من السمات الفسيولوجية ذات الاستقلال الجيني، وتحتوي على بنية فيزيائية غنية بالمعلومات للغاية ونمط نسيج فريد، وبالتالي فهي معقدة للغاية بما يكفي لاستخدامها كتوقيع حيوي. (Hosein 2005, 594-625) ، (Alan & Julia 2013) ، (Nabti & Bouridane 2008)

رابعا: الصوت: الصوت هو مزيج من القياسات الحيوية الجسدية والسلوكية. تعتمد سمات صوت الفرد على شكل وحجم الزوائد (مثل المسالك الصوتية والفم وتجويف الأنف والشفتين) المستخدمة في توليف الصوت ويعتمد نظام التعرف على الصوت المعتمد على النص على نطق عبارة محددة مسبقًا. يتعرف نظام التعرف على الصوت المستقل عن النص على المتحدث بغض النظر عما يتحدث به.

وهناك هندسة اليد والأصابع: من الملائم والمقبول للمستخدمين إجراء التعرف باليد. هناك العديد من ميزات اليد المتاحة للتعريف مثل هندسة اليد وبصمات الأصابع وبصمات راحة اليد وأوردة راحة اليد وما إلى ذلك(Hosein& Martin 2010) ، (Devereau & Vincent 2010)

المبحث الثالث

متطلبات بيانات البصمة البيومترية في الحوكمة الرقمية

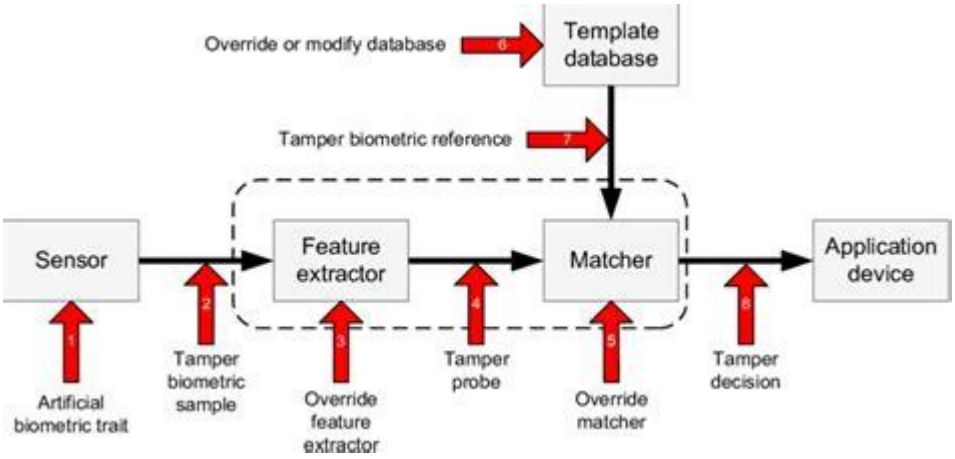
تم استخدام البيانات الحيوية على نطاق واسع في الطب الشرعي، مثل تحديد هوية المجرمين وأمن السجون، ولديها إمكانية أن يتم تبنيها على نطاق واسع في مجموعة واسعة جدًا من الخدمات الحكومية وكالاتي:

١. الأمن المصرفي، مثل التحويلات المالية الإلكترونية، وأمن أجهزة الصراف الآلي، وصرف الشيكات ومعاملات بطاقات الائتمان؛
٢. التحكم في الوصول المادي، مثل التحكم في الوصول إلى المطارات؛
٣. أمن نظام المعلومات، مثل الوصول إلى قاعدة البيانات عبر امتيازات تسجيل الدخول؛
٤. توزيع المزايا الحكومية، مثل برامج صرف الرعاية الاجتماعية؛
٥. أنظمة الهوية الوطنية، التي توفر هوية فريدة للمواطنين وتدمج خدمات حكومية مختلفة؛
٦. تسجيل الناخبين والسائقين، مما يوفر تسهيلات التسجيل للناخبين والسائقين
٧. الجمارك والهجرة، مثل نظام خدمة الركاب السريعة في دائرة الهجرة والتجنيس (INSPASS) الذي يسمح بإجراءات هجرة أسرع بناءً على هندسة اليد. ، (Digital Government Index 2019)

E-government Development Index) ، (Government Effectiveness Index 2021) (2022) .

٨. هجمات على الأنظمة البيومترية: الأنظمة البيومترية معرضة لأنواع مختلفة من الهجمات التي قد تعرض الأمن الذي يوفره النظام للخطر، مما يؤدي بالتالي إلى فشل النظام.

Figure (2): Possible attack points in a generic biometric system, inspired by Ratha

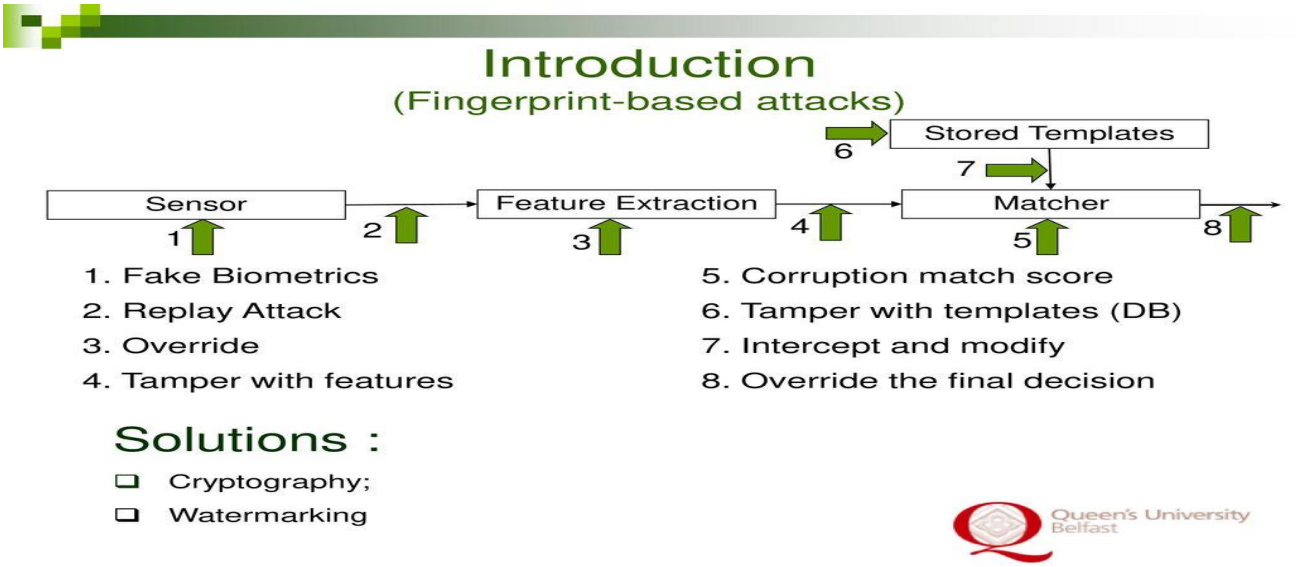


Source: https://www.researchgate .ne t/figure /Possible-attack-points-in-a-generic-biometric ...

وبخصوص موضوعة (الأنظمة القائمة على بصمات الأصابع) فانه تعتبر المصادقة القائمة على بصمات الأصابع هي التقنية الأكثر نضجًا وثباتًا واستخدامًا على نطاق واسع في جميع أنحاء العالم، نقاط ضعف الأنظمة القائمة على بصمات الأصابع: غير قابلة للاستبدال؛ غير سرية؛ قد تؤثر عدة هجمات محتملة على النظام البيو متري وتعتبر المصادقة القائمة على بصمات الأصابع هي التقنية الأكثر نضجًا وثباتًا واستخدامًا على نطاق واسع في جميع أنحاء العالم.

على الرغم من أن بيانات بصمات الأصابع توفر التفرد، إلا أنها لا توفر السرية لأن بيانات بصمات الأصابع هي: غير قابلة للاستبدال: لا يمكنك استبدال بصمة إصبعك غير سرية: على سبيل المثال، يمكنك ترك بصمة إصبعك على أي سطح تلمسه، ويمكن لأي شخص تسجيل صوتك أو الحصول على صورة لك. والأهم من ذلك كله أن الأنظمة البيو مترية قد تتعرض لتهديدات عديدة. وصف راثا وآخرون ثماني هجمات محتملة في النظام البيو متري . (Digital Government Index 2019) (Global Government Effectiveness Index 2021)، (Knowledge Index 2022).

Figure (2): Possible attack points in a generic biometric system, inspired by Ratha



Source: https://www.researchgate .ne t/figure /Possible-attack-points-in-a-generic-biometric ...

يتم تصوير عدة مستويات مختلفة من الهجمات التي يمكن إطلاقها ضد نظام القياسات الحيوية في (الشكل اعلاه). تهدف هذه الهجمات إما إلى التحايل على الأمان الذي يوفره النظام أو ردع الأداء الطبيعي للنظام.

١. سمة بيو مترية مزيفة، حيث يتم استخدام كائنات بيو مترية اصطناعية مزيفة أثناء عملية التحقق من الهوية. والسمة البيو مترية المزيفة هي إعادة إنتاج للسمة البيو مترية الأصلية وتحتوي على نفس الخصائص، مثل إصبع اصطناعي يمكن تقديمه إلى المستشعر؛ يقوم فرد غير مصرح له بتغيير سماته البيو مترية لتبدو وكأنها سمة مصرح بها.(Global Knowledge Index 2022)

٢. يتم اختراق البيانات البيو مترية للمستخدم المعتمد وإرسال هذه البيانات إلى النظام بشكل متكرر. ويؤدي ذلك إلى جعل النظام في حالة مشغول، بحيث لا يتمكن المستخدم الشرعي أبدًا من الوصول إلى خدمات النظام.

٣. و يتم تغيير برنامج مستخرج الميزات ببرنامج آخر يقوم بإنشاء مجموعات ميزات إخراجية محددة. وهذا يؤدي إلى تدهور أداء النظام وبالتالي فإن المستخدم الشرعي سوف يعاني أيضًا من مشكلة رفض الخدمة.

٤. يمكن استبدال مجموعات الميزات التي تم إنشاؤها بواسطة مستخرج الميزات بمجموعات ميزات أخرى أثناء نقل البيانات من مستخرج الميزات إلى المطابق. الآن سيحصل المطابق على مجموعة الميزات الاصطناعية بدلاً من مجموعات الميزات الشرعية.(EGovernment 2022)

٥. يمكن تغيير برنامج المطابق ببرنامج آخر تكون نتائجه صحيحة دائمًا. بعد ذلك، قد يكون لدى المستخدم غير المصرح له أيضًا إمكانية الوصول إلى النظام (Global Innovation Index" 2021)

المبحث الرابع

تقنيات البصمة البيو مترية: الأمان الرقمي وتحديات الخصوصية

اكتسبت تقنيات البصمة البيو مترية شعبية كبيرة وأهمية في مجال الأمن السيبراني. فهي توفر مستوى أعلى من الأمان والراحة مقارنة بأساليب المصادقة التقليدية. من خلال الاستفادة من السمات الفسيولوجية أو السلوكية الفريدة، يمكن للمؤسسات التحقق بدقة من هوية الفرد ومنح أو رفض الوصول وفقًا لذلك.

اولا: مزايا المصادقة الحيوية

توفر المصادقة الحيوية العديد من المزايا(Enhanced security 2021) منها:

١. تعزيز الأمن (Enhanced Security)

إن معرفات البيو مترية فريدة ويصعب تزويرها، مما يجعل من غير المحتمل للغاية أن يتمكن فرد غير مصرح له من الوصول إلى المعلومات الحساسة. حتى إذا سُرق قالب القياسات الحيوية، فلا يمكن استخدامه بشكل فعال لأنه يتطلب الوجود المادي للفرد.

٢. راحة المستخدم(User Convenience)

على عكس كلمات المرور أو أرقام التعريف الشخصية، والتي يمكن نسيانها أو إساءة وضعها، تعتمد المصادقة الحيوية على الخصائص التي يمتلكها الأفراد بشكل طبيعي. وهذا يلغي الحاجة إلى تذكر كلمات المرور المعقدة ويسمح بالوصول السريع والسلس.(Wendehorst & Duller 2021)

٣. منع الاحتيال (Fraud Prevention)

توفر البيومترية طريقة موثوقة لمنع الاحتيال على الهوية. من خلال التحقق من السمات الفريدة للفرد، يمكن للمؤسسات التأكد من أن الأشخاص المصرح لهم فقط لديهم إمكانية الوصول إلى المعلومات الحساسة، وبالتالي تقليل الأنشطة الاحتيالية.

ثانيا: التهديدات التي تواجه أمن البصمة البيومترية

على الرغم من أن البيو مترية تقدم مزايا كبيرة، إلا أنها ليست محصنة ضد التهديدات. ومن الأهمية بمكان فهم المخاطر المحتملة التي تتعرض لها الأنظمة الحيوية لضمان تدابير أمنية فعالة. وتشمل بعض التهديدات التي تواجه أمن المقاييس الحيوية ما يلي:

١. هجمات التزييف(Spoofing Attacks)

تتضمن هجمات التزييف إنشاء نسخة طبق الأصل أو تقليد السمات الحيوية للفرد للحصول على وصول غير مصرح به. ويمكن أن يشمل ذلك بصمات الأصابع المزيفة، أو التسجيلات الصوتية، أو حتى أقنعة الوجه ثلاثية الأبعاد. وتشكل تقنيات التزييف المتقدمة تحديًا للأنظمة الحيوية التقليدية.(Weinberg 2021)

٢. خروقات البيانات (Data Breaches)

البيانات الحيوية، مثل أي شكل آخر من أشكال المعلومات الشخصية، معرضة لانتهاكات البيانات. وإذا تعرضت قاعدة بيانات المقاييس الحيوية الخاصة بالمنظمة للخطر، فقد يؤدي ذلك إلى عواقب أمنية خطيرة. ويمكن استخدام البيانات الحيوية المسروقة لانتحال الهوية وسرقة الهوية. Van Canneyt (2019)

٣. مخاوف الخصوصية (Privacy Concerns)

يثير استخدام البيومترية مخاوف بشأن الخصوصية وحماية البيانات. وقد يتردد الأفراد في مشاركة البيانات الحيوية الحساسة بسبب مخاوف من سوء الاستخدام أو الوصول غير المصرح به. ويجب على المنظمات ضمان الشفافية والامتثال للأنظمة ذات الصلة للتخفيف من هذه المخاوف. Statista (2023)

ثالثا: الحلول الاساسية لتحديات الأمن البيو متري

لمواجهة التهديدات المرتبطة بالأمن البيو متري، تم تطوير حلول مختلفة:

١. اكتشاف الحيوية ((Liveness Detection))

يعد اكتشاف الحيوية تقنية تضمن أن العينة البيومترية المستخدمة للمصادقة مأخوذة من فرد حي وحاضر. يساعد هذا في منع هجمات التزييف من خلال اكتشاف ما إذا كانت العينة البيومترية المقدمة مأخوذة من شخص حي أو نسخة طبق الأصل ملفقة.(Statista. (2023)

٢. المصادقة متعددة العوامل ((Multi-Factor Authentication))

يضيف تنفيذ المصادقة متعددة العوامل جنبًا إلى جنب مع البيانات البيومترية طبقة إضافية من الأمان. يمكن أن يتضمن هذا مزيجًا من شيء يعرفه المستخدم (مثل كلمة المرور)، وشيء يمتلكه (رمز مادي)، وشيء هو (سمات بيومترية).

٣. المراقبة المستمرة ((Continuous Monitoring))

يمكن للمراقبة المستمرة للأنظمة البيومترية اكتشاف الأنماط غير العادية أو الشذوذ، مما يشير إلى خروقات أمنية محتملة. يمكن أن تتضمن المراقبة عوامل مثل سلوك المستخدم وسجلات النظام وأنماط الوصول، مما يضمن التعرف السريع والاستجابة للتهديدات.(Van Canneyt 2019)

٤. التخزين الآمن والتشفير ((Secure Storage and Encryption))

لحماية البيانات البيومترية من التعرض للخطر، من الضروري استخدام تقنيات التخزين الآمن وبروتوكولات التشفير. وهذا يضمن أنه حتى إذا تم الوصول إلى البيانات، فإنها تظل غير قابلة للقراءة وغير صالحة للاستخدام.(Weinberg 2021)

وفي عالم رقمي متزايد، فإن دور البيومترية في الأمن السيبراني أمر بالغ الأهمية. توفر المصادقة البيومترية طريقة آمنة ومريحة للتحقق من هويات الأفراد، مما يخفف من المخاطر المرتبطة بأساليب المصادقة التقليدية. ومع ذلك، فإن الأنظمة البيومترية ليست مضمونة، ويجب اتخاذ تدابير استباقية لمعالجة التهديدات المحتملة، مثل هجمات التزييف وانتهاكات البيانات. Wendehorst & Duller (2021)

رابعا: القيود المفروضة على الأنظمة البيو مترية

من خلال الاستفادة من حلول مثل اكتشاف الحيوية والمصادقة متعددة العوامل والمراقبة المستمرة والتخزين الآمن، يمكن للمؤسسات تحسين وضع الأمن السيبراني وحماية بياناتها الحساسة بشكل فعال

وقد يطرح التساؤل الموضوعي الاتي:

ما هي القيود المفروضة على الأنظمة البيو مترية ؟

على الرغم من أن الأنظمة البيو مترية أصبحت أكثر فعالية مع تقدم التكنولوجيا، إلا أنها ليست طريقة مضمونة للمصادقة أو التعريف. يتم توضيح بعض القيود المفروضة على الأنظمة البيو مترية أدناه وكالاتي:

١. الفشل في التسجيل

يحدث هذا عندما لا يمكن إنشاء قالب للمعلومات البيو مترية بنجاح. قد يكون هذا بسبب عدد من العوامل، مثل معلومات مرجعية منخفضة الجودة (على سبيل المثال، بسبب أجهزة الاستشعار أو الظروف البيئية السيئة – مثل الإضاءة – في وقت التسجيل)، أو قد يكون لدى الشخص حالة جسدية أو طبية

تمنعه من التسجيل في النظام. يعد ضمان معدلات التسجيل الفعالة أمرًا بالغ الأهمية للتشغيل الناجح لنظام التحقق أو المصادقة البيو مترية.(Wendehorst & Duller 2021)

بالإضافة إلى القضايا الفنية والظروف الجسدية أو الطبية، قد تحد العوامل الثقافية أو الدينية أيضًا من قدرة مجموعة أو فرد على المشاركة أو التسجيل في نظام بيو متري. على سبيل المثال، قد يُعتبر جمع صورة وجه أو نوع آخر من المعلومات الجسدية غير مناسب في بعض الثقافات أو الأديان. لا ينبغي التفكير في حدود التسجيل باعتبارها حواجز – بل يجب اعتبارها جزءًا طبيعيًا من مجتمع متنوع. يجب أن تكون المنظمات التي تستخدم الأنظمة البيو مترية حساسة لهذه الأمور عند طلب الأفراد لتقديم معلومات بيو مترية، ويجب على مصممي النظام التأكد من مراعاة هذا التنوع عند التخطيط لأي تنفيذ بيو متري. (Weinberg, A. (2021)

٢. معدلات القبول والرفض الخاطئة

يمكن أن ترتكب الأنظمة البيو مترية خطأين أساسيين. يحدث "الإيجاب الخاطئ" عندما يطابق النظام بشكل غير صحيح إدخالًا مع قالب غير مطابق، بينما في "السلبية الخاطئة"، يفشل النظام في اكتشاف تطابق بين الإدخال والقالب المطابق.(Zimmerman 2017)

هناك عدد من الأسباب التي قد تؤدي إلى حدوث مثل هذه الأخطاء في نظام بيومتري. قد يشترك أفراد مختلفون في خصائص بيو مترية متشابهة (على سبيل المثال، قد يكون من الصعب التمييز بين التوائم المتطابقة بناءً على القياسات الحيوية للوجه)، أو قد يختلف تفاعل المستخدم مع المستشعر بين مرحلتي التسجيل والتعرف (على سبيل المثال، قد يتخذ الشخص وضعية مختلفة).

ويمكن أن تؤدي عوامل أخرى مثل الشيخوخة أو الإصابة أو الظروف الطبية أيضًا إلى تغييرات في السمة البيو مترية للشخص بين مرحلتي التسجيل والتعرف.(Weinberg 2021)

إن مطابقة الفرد مع قالب مخزن في نظام القياسات الحيوية هو حساب احتمالي. وهناك هوامش للخطأ قد تتأثر بمجموعة من العوامل، بما في ذلك الخصائص العرقية أو العمرية لعينة البيانات المستخدمة عند تدريب النظام، أو الإضاءة أو وضعية الفرد في وقت التسجيل أو تحديد الهوية لاحقًا. إن العمل على تقليل معدلات الإيجابيات الكاذبة والسلبيات الكاذبة يشكل جزءًا مهمًا من تنفيذ أي حل للقياسات البيو مترية.Wendehorst& Duller, 2021)

تقدم القياسات الحيوية بعض المزايا لإدارة الهوية، إلا أن تحديد الهوية باستخدام القياسات الحيوية ليس حلاً مضمونًا ضد الاحتيال أو سرقة الهوية. وكما هو الحال مع تدابير الأمن الأخرى، فإن استخدام القياسات الحيوية به نقاط ضعف ويمكن اختراقه. على سبيل المثال، يمكن في بعض الأحيان إنشاء قطع أثرية مزيفة (مثل نسخة طبق الأصل من سمة بيو مترية) واستخدامها لخداع جهاز استشعار بيو متري. يُعرف هذا عادةً بالتزوير، ويمثل تحديًا لأمن الأنظمة الحيوية. نظرًا لأن الرؤية الحاسوبية تعمل بشكل

مختلف تمامًا عن الرؤية البشرية، فقد تكون بعض تقنيات التزوير غير بديهية في بعض الأحيان. (Zimmerman 2017).

ومن القيود الأخرى التي تفرضها الأنظمة البيو مترية أنه على عكس كلمات المرور أو رموز الهوية، لا يمكن إعادة إصدار أو إلغاء الخصائص البيو مترية. وإذا تعرضت بصمة إصبع الشخص أو أي من الخصائص البيو مترية الفسيولوجية الأخرى للخطر، فقد يكون من الصعب للغاية – إن لم يكن من المستحيل – تغيير هذه الميزة. وقد يكون هذا الأمر إشكاليًا عند استخدام هذه الخاصية البيو مترية للمصادقة في المستقبل.

ونظرًا للطبيعة المتطورة للقياسات البيو مترية، فإن التطورات الإضافية في مجالات مثل اكتشاف الحيوية والقياسات الحيوية القابلة للإلغاء قد تعالج بعض هذه القضايا والقيود التي تفرضها الأنظمة البيو مترية الحالية .(Zimmerman 2017)

تحتوي العديد من الأنظمة الحيوية على طرق لمحاولة مواجهة خطر التزوير، مثل اكتشاف الحيوية. اكتشاف الحيوية هو تقنية تستخدم لتحديد ما إذا كان مصدر العينة الحيوية هو إنسان حي أو تمثيل مزيف. على سبيل المثال، يمكن استخدامه للتمييز بين صورة حية وتمثيل مطبوع ثنائي الأبعاد أو ثلاثي الأبعاد لوجه شخص. ومع ذلك، حتى مع اكتشاف حيوية البيانات، قد يظل الحل البيو متري معرضًا لخطر الهجوم المعادي.

يقول نائب رئيس رابطة السفر الأمريكية للأمن والتيسير ريان بروبيس، يلاحظ موجة الأحداث الرياضية الدولية الضخمة التي ستقام في الولايات المتحدة في العقد القادم – بما في ذلك كأس العالم لكرة القدم ودورتين أوليمبيتين. يقول بروبيس إن إدارة التحديات الأمنية والتشغيلية التي تأتي مع تدفق الزوار ستتطلب أدوات جديدة ومنها فرض البصمة البيو مترية والتحقق البيو متري European Travel Information and Authorisation System (ETIAS) (

ويقول: "من المرجح أن يكون ثلاثة ملايين مسافر يوميًا هو القاعدة عندما تستضيف الولايات المتحدة كأس العالم في (١١) مدينة في جميع أنحاء البلاد"، مشيرًا إلى أن إدارة أمن النقل فحصت هذا العدد في يوم واحد فقط لأول مرة في عام ٢٠٢٤. ويصف بروبيس التكنولوجيا الحيوية بأنها "تغير قواعد اللعبة عندما يتعلق الأمر بأمن النقل"، ويقول إن الاستثمارات في الأنظمة الحيوية للمسافرين تشكل جزءًا أساسيًا من الحل.

ويقدم ملخصًا لطيفًا ومختصرًا لما يفعله برنامج إدارة أمن النقل الحيوي.

"أولاً وقبل كل شيء، تؤكد التكنولوجيا بيقين شبه مؤكد – أكثر من ٩٩ في المائة من الدقة – أن المسافر هو من يقول إنه هو.

ثانيًا، يتحقق هذا النظام من حالة الرحلة والفحص التي يخضع لها المسافر – فينبه ضابط إدارة أمن النقل إذا كان الفرد مسجلاً في برنامج (TSA Precheck) أو إذا كان يحتاج إلى فحص إضافي. وأخيرًا، يتضمن هذا النظام فحصًا شبه فوري لهوية المسافر من خلال قواعد بيانات الأمن الحكومية للقبض على المجرمين قبل أن يشكلوا تهديدًا للمسافرين.

تعتقد جمعية السفر الأمريكية أن عمليات التحقق البيومترية "أكثر فعالية واستدامة وقابلية للتطوير من محاولة توسيع البنية الأساسية وسعة التوظيف لاستيعاب حجم السفر المتزايد". وتحظى هذه العمليات بدعم شعبي: تستشهد المقالة باستطلاع حديث قال فيه أربعة من كل خمسة مسافرين إنهم يؤيدون استخدام التكنولوجيا البيومترية عند نقاط تفتيش أمن إدارة أمن النقل.

يوروستار في طليعة تبني تقنيات السفر الجديدة مع(iProov SmartCheck)يقدم مارك تشيلينجورث حجة مماثلة في مقالة لموقع (Diginomica)، حيث يزعم أن البيانات الحيوية ستلعب دورًا رئيسيًا في الانتقال إلى (ETIAS)والنشر النهائي لنظام الدخول والخروج البيومتري، ويعطي إشارة خاصة إلى يوروستار باعتبارها رائدة في تبني التكنولوجيا.

"لقد تأخر مرة أخرى تطبيق نظام الدخول والخروج الجديد للاتحاد الأوروبي والذي يستخدم البيانات البيومترية، لكن خبراء صناعة السفر يعتقدون أنه سيكون جاهزًا قبل صيف عام ٢٠٢٥. كما سيتم تقديم نظام (ETIAS) في عام ٢٠٢٥، حيث سيتعين على (٦٠) دولة من الدول المعفاة من التأشيرة الحصول على تصريح سفر لدخول ٣٠ دولة أوروبية." (ETIAS News & Information For Visitors Coming To Europe)

"لقد قامت شركة يوروستار بأكثر من مجرد الضغط على الحكومات"، يكتب تشيلينجورث؛ "لقد قامت شركة تشغيل السكك الحديدية بشراء وتنفيذ تقنية الحدود البيومترية بالشراكة مع شركة التكنولوجيا البريطانية ( ) iProovونظام(SmartCheck) الخاص بها. بدأت شركة يوروستار في استخدام (SmartCheck) في صيف عام ٢٠٢٣، بعد تجربة بين ديسمبر ٢٠٢١ وأبريل ٢٠٢٢."

يقول جاريث ويليامز، الأمين العام والمسؤول الرئيسي عن الشراكات الاستراتيجية لشركة يوروستار، إن إحدى فوائد استخدام(iProov) هي "استقلال البيانات؛ فأنت تتصل عند نقطة التسجيل، وتتصل مرة أخرى عندما تحتاج إلى السفر، وفي الأثناء، تظل البيانات معك. إنه يعادل اختيار تسليم جواز سفرك عند نقطة التحقق ثم إعادته إلى جيبك."

على الصعيد الأمني، يلاحظ تشيلينجورث أن (SmartCheck)يحتوي على ميزات تأخذ في الاعتبار التهديد الناشئ للذكاء الاصطناعي التوليدي والتزييف العميق المصمم لخداع محركات التعرف على الوجه. ويقوم النظام بإضاءة وجه المستخدم بسلسلة من الألوان المتغيرة بسرعة، وبينما يتم إضاءة الوجه،

يتم إرسال الفيديو مرة أخرى إلى خوادم(iProov) للتحليل الفوري" لاكتشاف القطع الأثرية الرقمية. (ETIAS News & Information For Visitors Coming To Europe)

الخاتمة :

تعتبر الحوكمة عنصرًا مهمًا آخر يجب مراعاته عند تبني واستخدام القياسات البيو مترية؛ إن الإشراف على الأنظمة والمساءلة عنها أمر بالغ الأهمية لضمان استخدامها بشكل مناسب.

ويجب أن يكون لدى الدول التي تستخدم الأنظمة البيو مترية أنظمة شكاوى واستفسارات شفافة، وتحديد السبل الداخلية والخارجية المناسبة للانتصاف، في حالة إساءة استخدام المعلومات البيو مترية أو وجود أخطاء في النظام البيو متري. من المهم أيضًا أن يتم توصيل عمليات الشكاوى وسبل الانتصاف هذه بوضوح للمستخدمين النهائيين.

وهناك تدبير آخر يجب مراعاته لتعزيز الحوكمة حول الأنظمة البيو مترية وهو تخصيص المسؤولية عن الإشراف على النظام لمسؤول كبير مناسب داخل المنظمة، والذي يتحمل المسؤولية عن تصميم وإدارة الخصوصية والأمان.

في مجتمع اليوم، يعد أمن البيانات مشكلة كبيرة لكل منظمة أعمال أو فرد. وأكثر التهديدات شيوعًا هو سرقة البيانات والمعلومات الشخصية. ومع مرور الوقت أصبحت البيانات الرقمية أكثر انتشارًا، ويحاول الموظفون تأمين معلوماتهم باستخدام كلمات مرور مشفرة للغاية وهويات مصادقة. ولكن إساءة استخدام وسرقة هذه التدابير الأمنية آخذة في الارتفاع في الكثير من حالات السرقة. ويؤدي الاستفادة من العيوب الأمنية في هويات المصادقة إلى تكرار أو تزوير البطاقات وبالتالي إساءة استخدامها. كانت هذه المعركة المتزايدة مع الأمن السيبراني السبب الوحيد وراء إنشاء أنظمة الأمن البيو مترية، والمجال المهم الذي يثير القلق هو كيف يمكن للمرء تنفيذ الأمن البيو متري لزيادة أمان البيانات. أول ميزة فريدة توجد بشكل مختلف في كل إنسان هي بصمات الأصابع، فقد استخدم البشر بصمات الأصابع للتعريف الشخصي. في الوقت الحاضر، تستخدم معظم المنظمات التعرف على بصمات الأصابع لعملية المصادقة، وهي واحدة من أقدم وأكثر القياسات الحيوية استخدامًا، بدقة عالية وسهلة وفعّالة وسريعة بشكل عام. في هذه الورقة نقترح فكرة استخدام التعرف على بصمات الأصابع جنبًا إلى جنب مع كلمة مرور مصادقة المستخدم للوصول إلى البيانات أو المعلومات. نظرًا لأن الشخص الوحيد الذي يمكنه الوصول إلى المعلومات هو الشخص المرتبط بها، فلا يمكن لأي لص الوصول إليها. كما يجعل ذلك من الصعب جدًا على مجرمي الإنترنت اختراق بياناتك.

إن التحقق من الهوية والمصادقة البيو مترية قد تقدم فوائد للقطاع العام، وخاصة في إدارة الهوية. وكما ذكر أعلاه، يمكن أن تكون المقاييس الحيوية وسيلة فعالة وموثوقة للتحقق من هويات الأشخاص، وبالتالي

يتم استخدامها في العديد من المجالات والقطاعات المختلفة، من أماكن العمل، إلى الدفع والخدمات المالية، إلى إنفاذ القانون. في بعض الحالات، يمكن للمقاييس الحيوية أيضًا تعزيز الخصوصية من خلال توفير مستوى أعلى من الأمان مقارنة بأشكال أخرى من التحكم في الوصول، مثل كلمات المرور أو بطاقات التمرير.

إن تنفيذ الأنظمة البيو مترية قد يحسن أيضًا من كفاءة العمليات الحكومية. إن تقنية التعرف على الوجه المستخدمة في البوابات الذكية في المطارات حول العالم هي مثال جيد على ذلك؛ حيث يتمكن الأفراد من معالجة دخولهم إلى بلد ما بدلاً من المرور عبر مسؤولي الهجرة والحدود. كما تم استخدام تقنية التعرف على الصوت كوسيلة للتحقق من هويات الأفراد عبر الهاتف عند الوصول إلى الخدمات الحكومية.

وفي العصر الرقمي والمعلوماتي، تقدم المقاييس الحيوية العديد من الفوائد والفرص لمنظمات القطاع العام لتحقيق أهدافها بطرق جديدة ومبتكرة، كما يتضح من الأمثلة المذكورة أعلاه. ومع ذلك، فإن لها أيضًا آثارًا على الخصوصية – وخاصة خصوصية المعلومات وبالمقابل فان جميع منافذ الدخول في دول الخليج العربي مجهزة بـ "النظام البيو متري".

الاستنتاجات:

بناء على ما عرضته الدراسة ومن واقع ما تناولته من تحديات بتوظيف تقنيات الذكاء الاصطناعي في التحقق البيو متري في دول العالم يمكن صياغة الاستنتاجات الاتية:

١. التحول الرقمي هو جوهر تكنولوجيا المعلومات وكل كل الدول ومنها العراق وضع خطة استراتيجية لتطبيقها بشكل فعال وتحدد رؤية العراق خارطة طريق شاملة للتحول الرقمي ، والتي تشمل الاستثمار في البنية التحتية الرقمية، وتعزيز الابتكار، وإنشاء نظام بيئي رقمي يدعم الشركات الناشئة ورواد الأعمال. من خلال تبني أحدث التقنيات وتعزيز ثقافة الابتكار والتعليم الرقميين، وتحدد خطة لتطوير قوة عاملة رقمية عالية المهارة يمكنها دفع التحول الرقمي في البلاد إلى الأمام. بشكل عام، وتحدد رؤية العراق المستقبلية خارطة طريق واضحة لمستقبل العراق الرقمي وتؤكد على التزام الدولة بالبقاء قادرة على المنافسة في الاقتصاد الرقمي العالمي. ويتحقق ذلك بالخطوات الاستراتيجية الاتية :

أ. وضع العراق كمركز للابتكار الرقمي وريادة الأعمال. من خلال إنشاء نظام بيئي داعم للشركات الناشئة ورجال الأعمال، يمكن للعراق جذب الاستثمارات والمواهب الدولية، وأن تصبح رائدة في الاقتصاد الرقمي العالمي.

ب. من خلال استخدام تقنيات المدن الذكية والحلول الرقمية التي تعمل على تحسين نوعية حياة المواطنين. يمكن استخدام التقنيات الرقمية مثل أجهزة الاستشعار وإنترنت الأشياء وتحليلات البيانات لمراقبة وإدارة العوامل البيئية مثل جودة الهواء وإدارة المياه وإدارة النفايات.

ت. من خلال الاستفادة من التقنيات الرقمية لتحسين تقديم الخدمات وتبسيط العمليات الإدارية. سيمكن التحول الرقمي الحكومة من تقديم خدمات أكثر فعالية وملاءمة للمواطنين، مما يقلل من عدم الكفاءة ويعزز الشفافية والمساءلة. رغم ذلك فانه هناك تحديات امام دولة الكويت تتعلق بالأمان الرقمي وتحديات الخصوصية.

٢. من أبرز تحديات البيو مترية للخصوصية بشكل عام، إن البيو مترية، مثل العديد من التقنيات الأخرى، قد تشكل تحديات للخصوصية. ومع ذلك، من المهم أن نلاحظ أن البيو مترية ليست غير متوافقة بطبيعتها مع الخصوصية؛ حيث إن كيفية تصميم الأنظمة واستخدامها تحدد مدى تعزيز البيو مترية لخصوصية الأشخاص أو انتهاكها لها. وفيما يلي بعض قضايا الخصوصية التي قد تنشأ عن استخدام البيو مترية.

٣. يحدث التسلل الوظيفي عندما تُستخدم المعلومات لغرض مختلف عن الغرض الذي جُمعت من أجله. ويصبح هذا مصدر قلق عندما لا يتم إبلاغ الفرد بالاستخدام الثانوي في وقت تقديم معلوماته. على سبيل المثال، قد تجمع إحدى المؤسسات معلومات بيو مترية عن وجه أحد الموظفين لأغراض المصادقة، مثل تمكين الوصول إلى مبنى وقد تُستخدم هذه المعلومات بعد ذلك لغرض ثانوي غير ذي صلة، مثل مراقبة أوقات بدء وانتهاء عمل الموظف.

٤. وهناك خطر آخر يهدد الخصوصية يتمثل في جمع المعلومات البيو مترية للأفراد سراً أو بشكل سلبي دون موافقتهم أو مشاركتهم أو علمهم. على سبيل المثال، يمكن التقاط المعلومات البيو مترية للوجه من الصور التي لا يعرف الأفراد أنها تُلتقط، ويمكن رفع بصمات الأصابع الكامنة لجمع المعلومات البيو مترية بعد فترة طويلة من ملامسة الفرد لسطح صلب.ويزداد هذا الخطر مع تقدم التكنولوجيات وفعاليتها في التقاط المعلومات البيو مترية بشكل غير واضح، أو من مسافة بعيدة.

المصادر باللغة الانكليزية:

1. Abdul Sattar, Aya Jaafar& Salih .Yusra Mahd . 2022. University of Baghdad College of Political Science .The position of Iraq in Russia's foreign policy after the year 2000 AD. Baltic journal of law & politics a journal of vytautas magnus university. Volume 15. Number 3.

2. Abed kadhim ,Hayder& Ibrahim , Shefaa Khaleel . 2022 . University of Baghdad. College of Political Science The Saudi Foreign Policy towards Iraq after 2014 University of Baghdad. College of Political Science. Iraq. Social science journal . vol.12. n3. November Issue.
3. Alan, Gelb & Julia, Clark. 2013."Identification for Development: The Biometrics Revolution." Center for Global Development. Working Paper 315. January.
4. All Ports of Entry in Kuwait Equipped with "Biometric System".May 29. 2023 ... As part of the security strategy to secure the border crossings with the latest security means and technologies. and in accordance with the . Available at: https://asmideast.com/all-ports-of-entry-in-kuwait-equipped-with-biometric -system /
5. Alrai .2011. Evaluation of Fingerprint Mechanism at the Airport. [Retrieved July 20th. 2011. Available at: :http://www.alraimedia.com/Alrai/Article_Print.aspx?id=274962 in Arabic
6. Al-Raisi, A and Al-Khouri. A. 2008. Iris recognition and the challenge of homeland and border control security in UAE. Journal of Telematics and Informatic. 25(2).
7. Alwan ,Saad Obaid .2022. University of Baghdad. College of Political Science Economic and security competition between the United States and Russia in Africa . Journal of Positive School Psychology . Vol. 6. No. 7.
8. Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Journal of Political Geography. 25(3).
9. 'Biometric system' activated at Kuwait's all ports of entry – ZAWYA. May 24. 2023 ... Citizens and residents must book an appointment through the "Meta" platform. and visitors through the Ministry of Interior's website. Available at:
10. Devereau. S. & Vincent. K.. 2010. Using technology to deliver social protection: exploring opportunities and risks. Development in Practice. Volume 20. Issue 3.
11. E-government Development Index (EDGI). 2022. [Online]. Available at: https://desapublications.un.org/sites/default/files/publications/2022-09/Web version EGovernment 2022.pdf.
12. Evrensel, A.. ed.. 2010. Voter Registration in Africa: A Comparative Analysis. Electoral Institute for Sustainable Democracy in Africa. Available at: http://www.eisa.org.za/PDF/vrafrica.pdf
13. Galbally, J. Alonso-Fernandaez. F. et al. 2012. A high performance fingerprint liveness detection method based on quality related features: Future Generation Computer System. 28 (1).
14. Gelb. A.. & Decker. C.. 2011. Cash at your fingertips: biometric technology for transfers in developing and resource-rich countries. Center for Global Development.
15. Government Effectiveness Index 2021. [Online]. Available at: https://www.theglobaleconomy.com/rankings/wb_government_effectiveness/.
16. Hosein, G.. and Martin. A.. 2010. Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations. The London School of Economics and Political Science. Available at: http://www2.lse.ac.uk/management/documents/electronic-health- privacy.pdf
17. Hosein, G.. and Nyst. C.. 2013. An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries. Privacy International. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229
18. Hosein, I. (2005). Transforming travel and border controls: Checkpoints in the Journal of e-Government Studies and Best Practices 20(4).

https://www.zawya.com/en/world/middle-east/biometric-system-activated-at-kuwaits-all-ports-of-entry-psnky1g7.
19. Journal of Research in Social Sciences and Humanities . (IJRSSH) Vol. No. 9. Issue No. IV.
20. KUNA: Kuwait taps biometric technology for improving border security.May 21. 2023 .The Interior Ministry announced Saturday introducing the biometric technology at all border crossing points as part of its strategy to use the latest . Available at: https://www.kuna.net.kw/ArticleDetails.aspx?id
21. Kuwait to share biometrics with Interpol. Gulf countries for regional.Mar 25. 2024 .Individuals can submit their biometric data at various Kuwait border outlets. including the Kuwait International Airport and designated centers . Available at: https://www.biometricupdate.com/202403/kuwait-to-share-
22. Liu, Y. 2009. The principle of proportionality in biometrics: Case studies from Norway. Journal of Computer Law and Security Review. 25 (3): 237-250.
23. McDowell, J..2000.Something You Are: Biometrics versus Privacy. Sans Institute. 2000-2002. Available at: http://www.giac.org/paper/gsec/2197/are-biometrics-
24. Nabti, M and Bouridane. A. (2008). An effective and fast iris recognition system based on a combined multiscale feature extraction technique. Journal of Pattern Recognition. 41 (3).
25. Namuq, Basma khaleel. 2019 . Identity reflection on the priorities of kurdish external political behavior: para diplomacy university of Baghdad. College of political science . International .
26. Noguchi M.. & Ueda H. (2021). An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures. NEC Technical Journal. 16 . Available at:https://www.nec.com/en/global/techrep/journal/g17/n02/170204.html
27. Poli, V. Arcot. N. & Charapanamjeri. J. 2009. Evaluation of Biometrics. IJCSNS International Journal of Computer Science and Network Security. 9 (9).
28. Roberts. C. 2005. Biometric. [Retrieved September 16th. 2011]. Available at: http://www.ccip.govt.nz/newsroom/infor mation-notes/2005/biometrics.pdf
29. Shaikh, S and Rabaiotti. J. 2010. Characteristic trade-offs in designing large-scale biometric-based identity management systems. Journal of Network and Computer Applications. 33(2).
30. Weinberg. A. 2021. Analysis of top 11 cyber attacks on critical infrastructure Analysis of top 11 cyber attackson critical infrastructure - FirstPoint /
31. Wendehorst. C.. & Duller. Y. 2021. Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces. Policy Department for Citizens' Rights and Constitutional Affairs EN Directorate-General for Internal Policies PE 696.968. Available at:https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf
32. Zimmerman. H. 2017. The data of you: Regulating private industry's collection of biometric information. U. Kan. L. Rev.. 66. 637.
33. Zreter, S. 2007. 'The right to registration: development. identity and social security' World Development. 35 (1).