أكتوبر 2022

إطلاق قوة البيانات عبر البيانات الاصطناعية الخاصة

faculty

دبـــــي الرقمية
DIGITAL DUBAI

فاكَلتي:

نحن في فاكَلتي نؤمن أن الذكاء الاصطناعي قادر على تغيير كل شيء، بما في ذلك التغلب على أهم تحديات المتعاملين لدينا، سواء كان المتعامل يبحث عن طريقة لتوفير الوقت أو تعزيز فاعلية العمل أو رفع مستوى الجودة لديه، فنحن نقدم تطبيقات رائدة في الذكاء الاصطناعي على مستوى العالم، بحيث تساهم في تحويل بيانات المتعاملين إلى حافز للإبداع ووسيلة لصنع قرارات مدروسة واستراتيجيات أفضل. ومع وجود نخبة من أفضل خبراء العالم في علوم البيانات (أكثر من 50 عضواً من الفريق يحمل شهادة دكتوراة من جامعة هارفرد، أكسفورد، وكامبريدج)، قمنا بمساعدة أكثر من 230 متعاملاً في استخدام الذكاء الاصطناعي لإحداث تطور غير مسبوق في مؤسساتهم.

مقدمة لشركة فاكلتي

تتكرر جداً مقولة (كليف هامبي) عالم البيانات المعروف بأن (البيانات هي النفط الجديد) ويجري الاستدلال بها بشكل متكرر خرج عن النطاق المقبول افقدها معناها الحقيقي، ولذا نرى أنه من الأصوب أن يُقال: مثل النفط ، تكون البيانات ذات قيمة ، ولكن إذا لم يتم تحسينها فلا يمكن استخدامها. ونحن نرى أن حماية الخصوصية هي العنصر الأبرز في عمليات معالجة البيانات لجميع المنظمات في العالم وخاصة الحكومات والمؤسسات العامة على وجه التحديد.

ولابد من الإشارة إلى أن سياسات الخصوصية نجحت حتى يومنا هذا وإلى حد كبير في حماية خصوصية البيانات ولكنّها في الوقت ذاته خلقت كلفة مهدورة باهظة وهي ومحدودية قابلية استخدام البيانات. فعلى سبيل المثال القيود الشديدة على الوصول للبيانات في هذه السياسات تقلل مخاطر خرق الخصوصية لكن في الوقت ذاته تحُد من فرص توظيف البيانات في معالجة المشكلات الخاصة بالسياسات العامة. وبصورة مشابهة مجموعات البيانات المدمجة تضمن خصوصيتها لكن تحدّ إلى مستوى معين من امكانية استخدام هذه المجموعات من البيانات في عمليات التحليل لخلق القيمة للأفراد والمجتمع.

وبناءاً على ماسبق فإننا نرى فرصاً في الجيل الجديد من معالجة البيانات وهو البيانات الاصطناعية الخاصة (private synthetic data)، حيث يتم توظيف نماذج الذكاء الاصطناعي لإيجاد مجموعات بيانات اصطناعية حقيقية ولكنّها خالية من البيانات الشخصية لكن تتميّز باحتفاظها بالدلالات والروابط الإحصائية بين المتغيرات في البيانات المتبقية للمعالجة.

هذا البحث الذي أجرته فاكلتي ودبي الرقمية يهدف لاستكشاف مدى الحفاظ على الخصوصية، وفي الوقت ذاته مدى قابلية البيانات الاصطناعية الخاصة للاستخدام في قوالب وتقنيات متعددة. وقد خلصنا في نتائج البحث إلى أن عملية (البيانات الاصطناعية الخاصة) تتيح مجموعات بيانات مناسبة جداً وبمستويات عالية للبحث وتلبي احتياجات السياسات العامة.

نتمنى لكم قراءة مفيدة للبحث، ونشكر دبي الرقمية لرعايتها هذا العمل البحثي، ومتشوقون لما سيقود إليه ونتائجه من فرص بمجال تحسين ممارسات الحفاظ على الخصوصية التي تتطلبها البيانات الخاصة وتجعلها قابلة للاستخدام من الحكومات حول العالم لخدمة البشرية.

الفهرس

لمحة عن هيئة "دبي" الرقمية - 2022

أطلق صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي هيئة دبي الرقمية في يونيو 2021 بهدف تطوير سياسات واستراتيجيات لتنظيم جميع القضايا المتعلقة بتكنولوجيا المعلومات والبيانات والتحوّل الرقمي والأمن السيبراني في دبي والإشراف على تنفيذها.

تضم هيئة دبي الرقمية خبرات أربع جهات حكومية تحت مظلتها وهي: مركز دبي للأمن الإلكتروني، ومركز دبي للإحصاء، ومؤسسة بيانات دبي ومؤسسة حكومة دبي الرقمية، وذلك لضمان تكاتف جميع الجهات المعنية بتحقيق رؤية قيادة المدينة بجعل دبي المدينة الرائدة عالميًا في مجال الاقتصاد الرقمي، وفي جعل دبي عاصمة رقمية عالمية.

تم تكليف هيئة دبي الرقمية بأربع مهام أساسية، هي: تسريع عملية التحوّل الرقمي في المدينة من خلال شراكات استراتيجية مع القطاعين الحكومي والخاص، وتعزيز الاقتصاد الرقمي في دبي، والعمل على بناء وتأهيل كفاءات بشرية رقمية، وأخيرًا المحافظة على ثروة دبي الرقمية وتطويرها مع تسريع وتيرة الجهود المبذولة في مجال الأمن السيبراني.

مؤسسة بيانات دبي

تم إطلاق "مؤسسة بيانات دبي" في العام 2016 بهدف بناء منظومة بيانات شاملة في المدينة. لتحقيق هذا الهدف تعمل المؤسسة اليوم على تطوير أربع ركائز أساسية، هي: حوكمة البيانات وهندسة البيانات وبنيتها التحتية والارتباط بالمنظومة والنقطة الأهم هي اعتماد مفهوم توليد القيمة.

خلال السنوات الخمسة الماضية، أصدرت مؤسسة بيانات دبي سياسات وإرشادات تشارك البيانات وتطابقها، ونشرت "مبادئ وإرشادات أخلاقيات الذكاء الاصطناعي"، وأنشأت "دبي بالس" الذي يشكل هيكل بيانات المدينة الأساسي ويستضيف اليوم أكثر من 900 مجموعة بيانات مشاركة ومفتوحة. كما أطلقت المؤسسة استراتيجية إشراك القطاع الخاص، وقامت ببناء لوحة بيانات خاصة بانتشار فيروس "كورونا - كوفيد 19" ومكافحته في المدينة بالشراكة مع مركز التحكّم والسيطرة لمكافحة فيروس "كورونا - كوفيد 19" في دبي.

مقدمة:
أهمية البيانات الاصطناعية

بناء منظومة متكاملة ومزدهرة تدعم الابتكار في مجال البيانات هي من اساسيات مهمة مؤسسة بيانات دبي. تعتبر القدرة على استخدام البيانات أمراً مهماً في منظومة البيانات، بحيث يمكن أن نخلق قيمة في مجتمع واقتصاد رقمي.

إن إنشاء وتوفير مجموعات البيانات الأكثر ثراءً وذات الصلة، والتي تغطي المزيد من مجالات الحياة والخدمات في المدينة، يبدو الان أكثر أهمية من أي وقت مضى. إدارة تحديات الصحة العامة المستمرة، وتأمين عودة الصحة الى الاقتصاد، والانتقال إلى اقتصاد خال من الكربون، بالإضافة إلى تغذية القطاعات الاقتصادية الجديدة "المتعطشة للبيانات" وأنظمةً الذكاء الاصطناعي التي ستنتشر مع دخولنا عصر الويب ٣.٠، كل هذا يتطلب الاستخدام الذكي للبيانات.

وبصفتنا الجهة المسؤولة عن بيانات إمارة دبي، ندرك تماماً أهمية القيمة الكامنة في البيانات الناتجة عن الحياة والقطاعات في المدينة، وفي الوقت ذاته نُدرك الحاجة للحفاظ على أمان وخصوصية بيانات الأفراد والمؤسسات التجارية والجهات الحكومية. لذلك قمنا بوضع سياسات ومعايير وإرشادات لتسهيل نشر وتبادل البيانات وضمان حسن استخدامها.

وانطلاقاً من مسؤوليتنا كقادة بيانات تقع على عاتقنا مهمّة استكشاف مفاهيم وممارسات جديدة لإدارة البيانات وحوكمتها وتحليلها، وهو ما يعزز مستويات الثقة والنشاط في سوق بيانات المدينةويرتقي بمستويات الابتكار في هذا المجال في الوقت ذاته. ولذلك اخترنا الشراكة مع (فاكلتي لعلوم البيانات Data Science) لتحقيق إنجاز جديد واكتشاف في مجال إعداد البيانات الاصطناعية .

وتأتي هذه الخطوة بالاعتماد على أدوات تبادل البيانات التي نشرناها العام 2020، والتي حققت نتائج واعدة، وقد أثبتنا عبرها أنه يمكننا إيجاد نُسخ مُركّبة خاصّة من مجموعات البيانات الحساسة المتوفرة، وعبر معالجة هذه البيانات الاصطناعية تمكّنا من المحافظة على السرّية وفي الوقت ذاته أبقينا على جزء لا يستهان به من المعلومات القيّمة التي تتضمنها مجموعات البيانات بحالتها الأولية، وبصورة تتيح التحليل المتقدم للبيانات ووضع نماذج لها وتصميم المنتجات القائمة على البيانات.

تفتح هذه التجربة الأولية الأبواب أمامنا بمؤسسة بيانات دبي فرصاً لا محدودة للكشف عن جوانب كامنة وغير مسبوقة ضمن مجموعات البيانات الخاصة بنا ومجموعات البيانات المتوفرة في الدوائر الحكومية بدبي، وكذلك يمكن لهذا النموذج أن يمتد ليشمل مؤسسات القطاع الخاص في المراحل المقبلة.

هذه المبادرة البحثية المتمثلة بالبيانات الاصطناعية الخاصة هي جزء من مبادرات أخرى عديدة، وتهدف جميعها إلى توفير حلول عالمية المستوى لإدارة البيانات وحوكمتها عبر سلسلة القيمة الكاملة للبيانات. ولابد من الإشارة إلى أننا نسعى عبر برنامج "سجلات دبي" إلى إنشاء أصول بيانات ممكنة لاتخاذ القرار الذكي تتميز بجودتها العالية والترابط فيما بينها. وأما على صعيد استخدام البيانات فإننا نتطلع لأن يكون توظيفنا للذكاء الاصطناعي في معالجتها أخلاقياً وعادلا، وهذا هو سبب قيامنا بتعزيز مجموعة أدوات التقييم الذاتي الأولية الخاصة بنا.

وانطلاقاً مما سبق، فإن هذا البحث يأخذ بالحسبان الجوانب الاقتصادية والاجتماعية في الوقت ذاته الذي يركّز على الجوانب التقنية المطروحة فيه. ولا يخفى على أحد أن هذه المرحلة الحاسمة التي تعيشها البشرية تتطلب أن تتركّز دراسات ومناقشة البيانات في المدن على هذه الجوانب، وكلّنا ثقة أن هذا البحث خطوة مهمة في هذا الاتجاه.

01

كيف تُقرأ
هذه "الورقة البحثية"

كيف تُقرأ هذه "الورقة البحثية"

تستهدف هذه الورقة البحثية فئتين من الجمهور– قادة البيانات الحكومية المهتمين في إدارة البيانات بشكل عام ومخرجاتها، أما الفئة الثانية فهم خبراء علوم البيانات. **وفيما يلي التفاصيل:**

خبراء علم البيانات

وهم الباحثون عن معلومات تقنية تفصيلية حول تقنيات الخصوصية وحماية للبيانات الحالية، وعن شرح مفصّل لنتائج البحث لمعرفة كيف تؤثر تقنيات الخصوصية (differential privacy techniques) ومدى فعاليتها في حماية خصوصية مجموعات البيانات

قادة البيانات

وهم الباحثون عن معلومات تقنية تفصيلية حول تقنيات الخصوصية وحماية للبيانات الحالية، وعن شرح مفصّل لنتائج البحث لمعرفة كيف تؤثر تقنيات الخصوصية (differential privacy techniques) ومدى فعاليتها في حماية خصوصية مجموعات البيانات

بناء على ما سبق، فقد تم تصميم هذه الوثيقة بطريقة تخدم كلا الفئتين كما يلي:

الجزء	العنوان	الوصف	الفئة المستفيدة
2	**تحويل الابتكار إلى قيمة عمليّة: البيانات الاصطناعية الخاصة**	شرح مفصّل للفرص المتاحة أمام المؤسسات وقادة بيانات المدينة عند استخدام البيانات الاصطناعية الخاصة، مع موجز عن خلفية البحث وتفاصيل البحث ذاته.	◐ الجميع
3	**تأثير البيانات الاصطناعية الخاصة على خصوصية البيانات**	نقاش حول تطور البيانات الاصطناعية الخاصة وكيف أصبحت أداة فعالة تُحقق التوازن بين الخصوصية وصلاحية البيانات الحساسة للاستخدام.	◐ الجميع
4	**شرح غير تقني مفصّل حول البحث ومخرجاته**	شرح غير تقني مفصّل حول منهجيتنا في البحث والنتائج والمخرجات.	● القادة الحكوميون
5	**مراجعة فنية للتقنيات الحالية**	مراجعة لعدة تقنيات متوفرة حالياً في دراسات ومؤلفات التي توضّح كيفية تعزيز خصوصية الأفراد في البيانات الصادرة، وحماية الخصوصية من أي انتهاك.	○ الخبراء الفنيون
6	**شرح تقني لآلية عملنا والنتائج**	نقاش فني حول منهجيتنا الاختبارية المتبعة من أجل تقييم العلاقة بين سهولة وفعالية الاستخدام والخصوصية ضمن آليات إصدار البيانات المختلفة.	○ الخبراء الفنيون
7	**المراجع**	قائمة بالمراجع المستخدمة في تحضير هذا البحث.	–
8	**الملحق التقني**	لمحة عن مجموعات البيانات المستخدمة والمزيد من التفاصيل حول التجارب المبينة في الجزء 6.	○ الخبراء الفنيون

02

تحويل الابتكار إلى قيمة عمليّة:
البيانات الاصطناعية الخاصة

تحويل الابتكار إلى قيمة عمليّة: البيانات الاصطناعية الخاصة

يتناول هذا الجزء:

أهمية البحث في البيانات الاصطناعية الخاصة.

شرح موجز عن البحث.

فرصة المؤسسات وقادة بيانات المدينة المرتبطة بالبيانات الاصطناعية الخاصة.

ما أهمية هذا البحث؟

"دبي بالس" هي منصة بيانات إمارة دبي، وكغيرها من المنصات، فإنها تحتوي على تنوع هائل من البيانات التي يمكنها توفير حلول لأي تحديات تواجه وضع السياسات العامة، وتوفير خدمات أفضل وتحفيز الإبتكار باستخدام تقنيات جديدة بشكل عام.

وليس غريباَ أن غالبية مجموعات البيانات في المدينة تتميّز بكونها حساسة لأسباب وجيهة، فبعضها سرّي من الناحية التجارية، وقد يؤدي أي تهاون في التعامل معها لجعلها منفذاً يعرّض الأفراد والبنى التحتية المهمة للمدينة للمخاطر. ولذا قمنا بتسليط الضوء على أهمية وضع ضوابط لضمان عدم تسرب هذه البيانات أو إساءة استخدامها.

بناء عليه، فإن توفير مجموعات بيانات ضخمة ومفصّلة بحيث تكون متاحة لإجراء عمليات تحليل متقدمة وتوظيف تقنيات الذكاء الاصطناعي يبشر بنتائج ومخرجات متعددة وقيمة أكبر في مجالات اجتماعية وبيئية واقتصادية مهمة لهذا العصر، كما بات البحث عن طرق جديدة لجعل تلك البيانات متاحة لتمكين مستخدميها من المهتمين من خلق القيمة مع المحافظة على الخصوصية، مع الامتثال لقوانين الأمان والحماية الصارمة أمراً في غاية الأهمية.

البحث

تُستخدم مجموعة متنوعة من تقنيات إخفاء الهوية بكثرة في عمليات حوكمة المعلومات، والتي تعمل على ضبط الوصول إلى مجموعات البيانات المخزّنة في "دبي بالس". وقد قمنا خلال هذا البحث باختبار هذه التقنيات ومقارنتها مع التحديثات الجديدة في مجال إنتاج البيانات الاصطناعية (synthetic data)، على وجه التحديد البيانات الاصطناعية الخاصة الناشئة باستخدام تقنيات الخصوصية التفاضلية (differential privacy).

البيانات الاصطناعية	هي بيانات تمّ إعدادها اصطناعياً من مجموعات البيانات الأصلية وبشكل تحافظ فيه على معظم الخصائص الإحصائية لمجموعة البيانات الأصلية دون نسخ أو تضمين الحقول الخاصة بالأفراد والتي تتيح التعرّف عليهم منها.
الخصوصية التفاضلية (Differential privacy)	هي إطار عمل حسابي محكَم يهدف إلى الحد من الكشف عن المعلومات الإحصائية وضبط مخاطر الخصوصية. ببساطة، وهي آلية تسمح للمستخدم بتحقيق نتائج تحليل واستدلالات إحصائية بنفس الإمكانيات التي تتيحها البيانات الكاملة ولكن مع فارق عدم القدرة على تحديد الجوانب الفردية مثل بيانات الأفراد أو التعرف عليهم.
بيانات الاصطناعية الخاصة (Private-synthetic data)	هي نوعٌ محدد من البيانات الاصطناعية والتي تنتج عن تطبيق تقنيات الخصوصية التفاضلية (differential privacy).

لإتمام البحث قمنا بمجموعة من الاختبارات على آلاف السجلات ضمن مجموعات البيانات، بما فيها بيانات الحوادث المرورية المسجلة في "دبي بالس". وخلال التجارب تمت مقارنة حجم الخصوصية المتوفرة ومرونة وقابلية الاستخدام في مجموعات البيانات مع هذه التقنيات مقارنة مع آليات العمل التقليدية.

وقد أظهر البحث أن البيانات الاصطناعية الخاصة (private-synthetic data) تتفوق في الأداء على التقنيات التقليدية لإخفاء هوية البيانات (من حذف أو تبديل أو تغطية حقول معينة أو تجميع) سواء في حماية خصوصية الأفراد أو تعزيز مرونة استخدام البيانات (أو أهميتها). وبالنسبة لمجموعة بيانات الحوادث المرورية في "دبي بالس" فقد تمكّنا من حماية خصوصية الأفراد بشكل شبه كامل مع المحافظة على نسبة 90% من قابلية البيانات للاستخدام ومرونتها، وذلك بالمقارنة مع مجموعة البيانات الأصلية.

هذه المخرجات، إلى جانب إمكانية الضبط الدقيق للخصوصية ومرونة الاستخدام التي لم تتمكن من تحقيقها التقنيات التقليدية، تجعل من الخصوصية التفاضلية (differential privacy) بديلاً مثالياً وضرورياً وقاعدة ذهبية في حماية خصوصية البيانات.

قادة بيانات المدينة يرجى الرجوع إلى الجزء 4 لتفاصيل الشرح غير التقني لطريقة العمل والنتائج.

خبراء علوم البيانات يرجى الرجوع إلى الجزء 6 للشرح التقني المفصّل حول طريقة العمل والنتائج.

الفرصة: تحويل الابتكار إلى قيمة عمليّة

بالنسبة للمؤسسات، يمكنها الاستفادة من مجموعات البيانات الاصطناعية الخاصة في النواحي التالية:

تقليل مخاطر انتهاكات وتسريبات البيانات الخاصة بالمؤسسة

المشاريع التي فشلت في السابق بسبب التخوّف من المساس بسرية البيانات **أصبحت ممكنة** الآن.

الحد من مخاطر الضعف أو الخلل في إنجاز وتسليم المشاريع التي تعتمد على بيانات سرية أو حساسة، حيث تتيح التقنيات الجديدة هنا عمليات التحليل حسابياً على بيانات ممثلة (بدلاً من طرق الحفاظ على السرية التقليدية مثل تبديل البيانات أو تغطيتها بشكل مفرط).

التقليل من تكلفة تسليم المشاريع، حيث تخضع إدارة المعلومات واستخدام البيانات **لقيود أقل.**

أي أن **الفائدة الكلية** للمؤسسات تتمثل بتمكين الجهات من الاستغلال أفضل لبياناتها في مجال تحليل البيانات وعلومها، إضافة إلى تنفيذ مشاريع أكثر تعقيداً باستخدام الذكاء الاصطناعي، وهو ما ينعكس إيجاباً على ثقافة المؤسسة حكومية أو خاصة وممارساتها لأعمالها.

الاستثمار

كي تستفيد المؤسسات من الخصوصية التفاضلية (differential privacy) عليها الاستثمار في الأدوات الصحيحة والمهارات المناسبة لتطبيق تلك التقنيات بصورة فاعلة على مجموعات البيانات.

فيما يتعلق بالأدوات المستخدمة في الخصوصية التفاضلية، يمكن استخدام مزيج من المصادر المفتوحة (مثل مكتبة جوجل للخصوصية التفاضلية (Google's Differential Privacy Library) ومنصة هارفرد "OpenDP") والاستفادة من البرامج التي تحتاج لتراخيص المتوفرة في سوق البرمجيات.

ويعتمد اختيار الأدوات المناسبة على حالة الاستخدام، مثلاً:

في بعض الحالات، قد يكفي استخدام **مكتبات المصادر المفتوحة** (مثلاً لتوليد إحصاءات تجميعية باستخدام الخصوصية التفاضلية)

في حالات أخرى (مثل تدريب خوارزميات تعلم الآلة) قد تتطلب شراء **برمجيات تجارية متخصصة.**

في حالات الاستخدام التي تتطلب برمجيات مرخّصة، قد تشكل تكلفة البرمجيات عائقاً أمام البدء، لكن مع انتشار وشيوع استخدام تلك التكنولوجيا (حسب قانون مور) فإن التكلفة ستنخفض تدريجياً. لذلك ننصح المؤسسات بإعطاء الأولوية لحالات الاستخدام الأكثر أهمية والأكبر تأثيراً من أجل تحقيق عائد أكبر على الاستثمار.

مهما كانت الأداة التي تختارها المؤسسة للاستثمار فيها، لا بد أن يرافقها الاستثمار في تنمية المهارات، فوضع الخصوصية التفاضلية في غير مكانها قد ينتج عنه عواقب وخيمة على مستوى المؤسسة والأفراد. في حالات استثنائية قد لا تخسر المؤسسة قيمة الاستثمار فحسب، بل قد يؤدي الأمر إلى غرامات ضخمة في حالة حدوث انتهاك لأي من قوانين الخصوصية، لذا من أجل ضمان تنفيذ تلك التقنيات بنجاح حسب حالة الاستخدام، يجب أن يتوفر فريق ماهر من الخبراء وعلماء البيانات.

أثناء العمل لاتخاذ القرار حول جدوى الاستثمار في هذه التكنولوجيا، من المهم جداً أخذ أهمية ومميزات الخدمة التي نقوم بتصميمها بعين الاعتبار. فإذا ما كان للخدمة قيد التصميم فائدة واضحة (مثل تحقيق الإيرادات، تخفيف التكلفة، توفير منتج جديد)، حينها قد يكون الاستثمار في هذه التقنية منطقياً من أجل تحقيق تلك الغايات، مع مراعاة أن هذا القرار يجب دراسته وأخذه بناءً على كل حالة الاستخدام بشكل منفرد.

الفرص المستقبلية لإدارة بيانات المدينة

تمثل فرصة توفير بيانات اصطناعية خاصة كخدمة للقطاعين الخاص والحكومي في دبي رؤية مستقبلية ملهمة، بما تحمله من فائدة عظيمة في منظومة حيوية واسعة النطاق.

ويفتح هذا البحث التقني فرصة حقيقية أمام مؤسسة بيانات دبي لتنفيذ استراتيجية على أربع مراحل من أجل توسيع نطاق استخدام البيانات الاصطناعية الخاصة بناء على فوائد المشاريع والأعمال.

إنشاء مجموعات بيانات اصطناعية خاصة	بيانات اصطناعية مفتوحة على "دبي بالس"	بيانات اصطناعية خاصة كخدمة	بيانات اصطناعية خاصة كخدمة
لدبي الرقمية	لدبي الرقمية	للحكومة	لمدينة دبي
إنشاء نسخ اصطناعية خاصة من مجموعة بيانات مختارة هامة من "دبي بالس"	نسخة اصطناعية من "دبي بالس" تحول مجموعة البيانات المحدودة إلى مفتوحة (حسب الملاءمة) مع الحفاظ على الترابط الكامن بينها	تفتح بيانات اصطناعية خاصة لتستخدمها الجهات الحكومية في دبي أو الإمارات الأخرى	توفير خدمة بيانات اصطناعية خاصة لكل إمارة دبي مع إمكانية جعلها إلزامية في بعض المجالات الحيوية

الشكل 1: استراتيجية بيانات مبنية على بيانات اصطناعية مفتوحة

توظيف هذه التكنولوجيا في **إمارة دبي سيجعلها تقود العالم في مجال حماية البيانات؛**

وذلك بتطبيق آلية عمل توظف التكنولوجيا لاكتساب الثقة مع فتح المجال أمام الابتكار، بدلاً من الاعتماد على تشريعات تمنح الثقة من خلال تقييد الابتكار.

فرصة فورية على مستوى إدارة بيانات المدينة

تعدّ البيانات الاصطناعية فرصة لمؤسسة بيانات دبي، حيث ستتمكن مباشرة من تحديد قيمة بياناتها المشتركة وبالتالي أهمية منصة "دبي بالس". وذلك يعني:

منصة "دبي بالس" مفتوحة بشكل فعلي

أي مساعدة مؤسسة بيانات دبي في تحقيق غايتها بجعل دبي المدينة الأسعد على وجه الأرض من خلال إتاحة المنصة لسكان وقادة المدينة سواء في القطاع الحكومي أو الخاص.

زيادة الخدمات المبنية على البيانات

أي زيادة عدد الخدمات الرائدة المبنية على البيانات لمواطني وقادة المدينة من خلال توفير المزيد من البيانات للأفراد، مثل استخدام النسخ الاصطناعية في السجلات الطبية للمساهمة في توقّع إعادة إدخال المرضى.

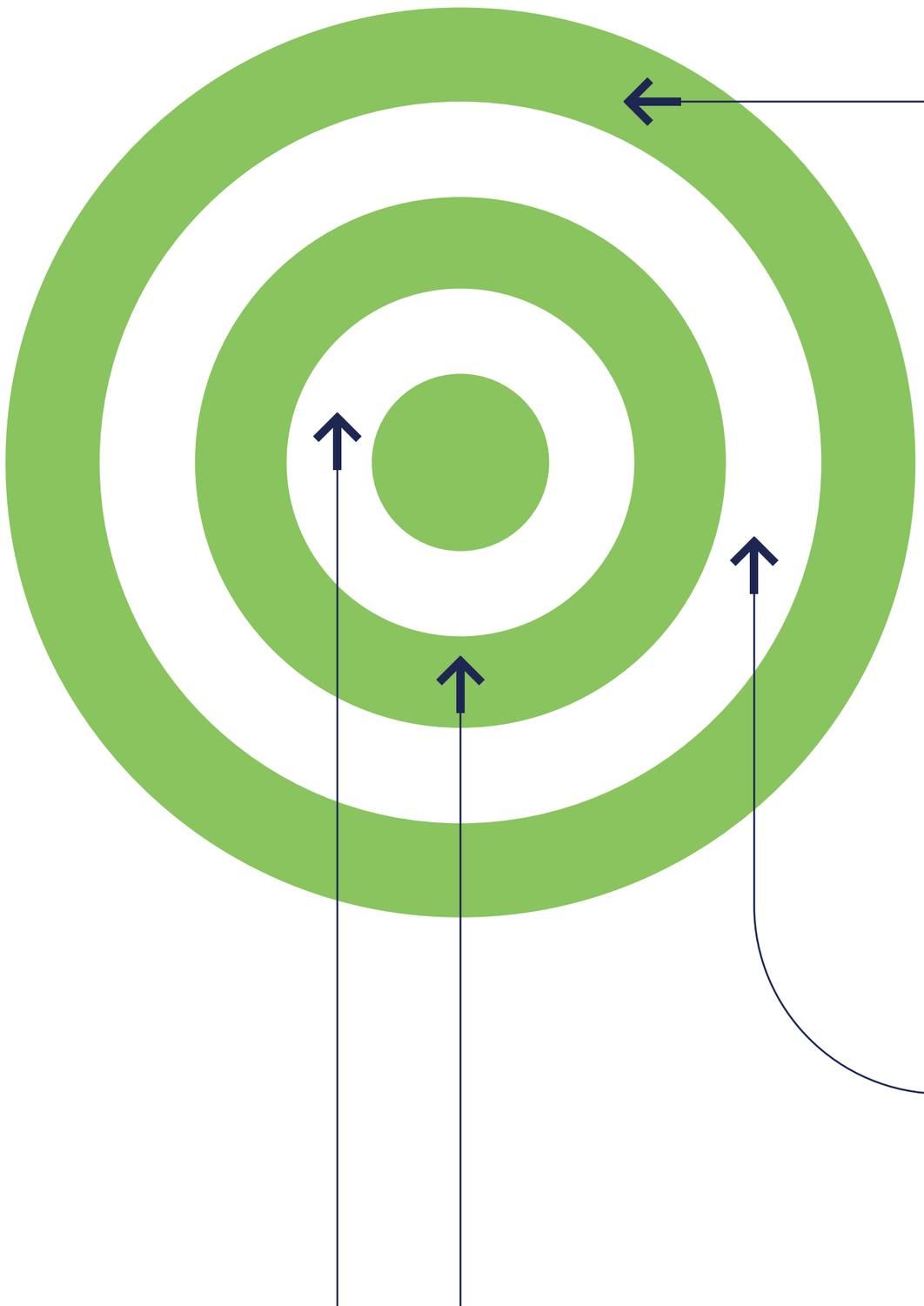
تنسيق تحليل البيانات بين القطاعين العام والخاص

حيث تملك البيانات الاصطناعية القدرة على تحديد القيمة المحتملة لدمج مجموعات بيانات من القطاعين العام والخاص. مثلاً يمكن دمج بيانات الاتصالات مع بيانات الاستخدام لسيارات الأجرة ليساعد في تحديد مواقع وجود مواقفها.

- تحليل البيانات بطريقة أقل تعقيداً وأكثر أماناً

فمن خلال تطبيق الخصوصية لبيانات اصطناعية بشكل حسابي، يمكن اتخاذ قرارات مدروسة بخصوص مشاركة مجموعات البيانات السرية والحساسة، كما يساهم توفير نسخ اصطناعية للبيانات الحقيقية في الحد من الحاجة إلى مجموعات بيانات تتألف من معلومات سرية أو حساسة تحتاج لدراسة كل حالة استخدام على حدة.

حالات استخدام جاهزة للتركيز عليها



بيانات السجل الطبي للمريض.

وتتألف من عدد من مجموعات البيانات ذات محتوى كبير من المعلومات حول المريض كالتاريخ الطبي ورحلته في مرافق المدينة الطبية. ومن المعروف أن الوصول لهذه البيانات محظور بالكامل كونها سرية وحساسة، وبالتالي هناك فرص تحليلية كبيرة سواء في مجال التطبيقات السريرية أو الإجرائية.

كما أن هذه الحالة شديدة الأهمية نظراً لوضع جائحة كوفيد19-. حيث يمكن استخدام تلك البيانات لدراسة طرق انتقال العدوى ومعرفة مضاعفاته وتحليل خيارات علاجية أكثر فعالية. ويمكن من خلال استخدام البيانات الاصطناعية الخاصة توظيف البيانات الفعلية في فهم الفيروس أكثر مع الحفاظ على خصوصية المريض في الوقت ذاته. مثلاً، يمكن استخدام البيانات في بناء نموذج لتأثيرات طرق العلاج المتعددة من أجل توفير رعاية أكثر تخصصية والتمييز بين الممارسات الصحيحة والخاطئة. كما يمكن استخدام البيانات للتنبؤ بهوية المرضى الذين يواجهون درجة عالية من المخاطر من أجل إعادة العدوى وإعادة الادخال الى المركز الصحي.

حالات استخدام جاهزة للتركيز عليها (في الإدارة العامة للإقامة وشؤون الجانب).

تحتوي مجموعة البيانات هذه على معلومات حول المقيمين في دبي مثل تاريخ الولادة والسجل الأكاديمي والوظيفة الحالية. والحصول على هذه المعلومات محظور بالكامل كونها سرية وحساسة. في حين أنه يمكن استخدامها لبناء ملف غني حول العرض والطلب للمهارات التي تساهم في تعزيز النمو الاقتصادي للمدينة. كما يمكن إجراء تحليل لها لمساعدة أصحاب القرارات في ضمان توفر المهارات اللازمة لتحقيق الرؤية الصناعية المستقبلية في دبي.

مواقع تحميل وتنزيل ركاب سيارات الأجرة.

تحتوي مجموعة البيانات هذه على تفاصيل الوقت والمكان المتعلقة بتحميل وتنزيل الركاب في دبي، وهي مصنفة بأنها سرية في الوقت الحالي. علماً بأنه يمكن استخدام تلك المعلومات لبناء نموذج حول تدفقات الركاب وحركة المرور في المدينة، وقياس مدى التأثير لأي تغييرات في الإنشاءات والطرق الجديدة وغيرها من أعمال التطوير. كما يمكنها المساعدة في فهم وتحديد مدى تأثير الفعاليات الضخمة التي تعتبر محوراً أساسياً في استراتيجية دبي الاقتصادية.

"بيانات الاتصالات" (حركة الاشخاص).

وتحتوي هذه المجموعة على بيانات حسابات لمشتركي دو وفقاً للتنوّع الديموغرافي السكاني في الإمارة. واستخدام هذه البيانات محظور بالكامل كونها سرية. وكما هو الأمر في حالة بيانات تحميل وتنزيل ركاب سيارات الأجرة، فإن هذه البيانات تصلح للاستخدام في بناء نموذج لتركيز السكان في المدينة، الأمر الذي يوفر مزايا ذكرناها سابقاً ويضاف لها المساهمة في الإدارة الاستباقية للتجمعات والحشود. ومع وجود عدد كبير من الفعاليات في دبي، يمكن لتلك المعلومات أن تفيد منظمي الفعاليات وهيئات تطبيق القانون على وجه التحديد.

آثار على مستوى الحوكمة

تثير البيانات الاصطناعية تحديات في مجال الحوكمة وإدارتها، فنشر وتوزيع البيانات الاصطناعية يجب أن يكون منسجماً لإدارة ومعايير حوكمة البيانات الخاصة بنا، والتي تتمحور حول التبادل الآمن والسهل والعادل والموثوق للبيانات. لذا يجب وضع معايير لإنتاج واستخدام وتصنيف البيانات الاصطناعية . كما كما من الارجح ان يتم تعديل نظام تصنيف البيانات الحالي (البيانات المفتوحة، والمشتركة، والحساسة والسرية)، مع مراعاة أن البيانات من الفئات الثلاث الأخيرة ستمر بتغييرات وأصبحت الآن بيانات مفتوحة أو على الأقل أكثر قابلية للتبادل بصورة اصطناعية.

وقد أوردنا في هذا التقرير مجموعة من الأمثلة لحالات استخدام البيانات الاصطناعية في القطاع الخاص. لكن يجب الإقرار بأننا لا زلنا في مرحلة مبكرة من تطبيق البيانات الاصطناعية في ممارسات إدارة البيانات للقطاع العام، كما أن جعل البيانات الاصطناعية متاحة للاستخدام عبر نظام البيانات، مثل نظام بيانات اصطناعي مفتوح على "دبي بالس" سوف يرفع من سقف التحدي.

كما أن المفاضلة بين الخصوصية وقابلية استخدام البيانات، وكيفية التعامل مع الأمر بشكل مختلف حسب كل حالة استخدام، سوف يشكل تحدياً في البداية دون أدنى شك. ففي بعض الحالات، يمكن القبول بدرجة منخفضة من الخصوصية، لكن في حالات أخرى تكون نسبة احتمال إعادة تعريف بيانات تجارية أو شخصية حساسة معدومة. وفي كل الحالات، كل عملية استخدام وإعادة استخدام محددة بدقة لها قدر من الامتيازات والصلاحيات.

هذه العوامل المذكورة أعلاه تبرز ضرورة وضع معايير توجّه اتخاذ القرارات مثل "متى نستخدم البيانات الاصطناعية " وبالتالي "كيف نستخدمها بشكل صحيح في حالات معينة". وهذه الخطوة بحد ذاتها تتطلب إجراء التجارب خلال المرحلة الأولية على تقنيات (Sandboxing) لتأثيرات برمجية تكنولوجية وإدارية.

وبناء على مخرجات هذه التجارب، يمكننا النظر في منح علامة الثقة لبيانات اصطناعية في القطاع العام والخاص لتشجيع استخدامها –كما قمنا بذلك مسبقاً على أنواع أخرى للبيانات، وفي نهاية الأمر يمكننا الإقرار إذا ما كان هذا النوع من الأنشطة يتفاعل مع نظم حوكمة البيانات الأخرى مثل أنظمة الذكاء الاصطناعي التي تستخدم هذه البيانات كأساس في اتخاذ القرارات.

03

تأثير البيانات الاصطناعية الخاصة على خصوصية البيانات

تأثير البيانات الاصطناعية الخاصة على خصوصية البيانات

يتناول هذا الجزء:

سبب تحول خصوصية البيانات إلى عقبة أمام الحكومات حول العالم

تقنيات حماية الخصوصية الأكثر استخداماً

ظهور البيانات الاصطناعية وعلى وجه التحديد البيانات الاصطناعية الخاصة المصممة وفق الخصوصية التفاضلية (differential privacy) كحل فاعل لتشجيع الابتكار المبني على البيانات وحماية الخصوصية.

نشأة البيانات الاصطناعية

التقنيات التي تُخطط هيئة دبي الرقمية لتوظيفها ضمن أهدافها طويلة الأمد تتطلب كمية ضخمة من البيانات، وذلك يتماشى مع زيادة إنتاج البيانات المتسارع حول العالم. فوفقاً للمنتدى الاقتصادي العالمي، فإن البشر في طريقهم لإنتاج 44 زيتابايت من البيانات بحلول 2020، بعد تراكم 4.4 زيتابايت فقط (أي 4.4 مليار تيرابايت) من البيانات في عام 2013 (المنتدى الاقتصادي العالمي 2019).

وكما ازداد جمع البيانات، ازداد أيضاً الوعي بالتحديات المتعلقة بحماية الخصوصية وأهميتها. فالحفاظ على أمن البيانات اليوم تحدٍّ حقيقي، وذلك لكثرة البيانات المعرّضة للضياع أو السرقة أو سوء الاستخدام أو الكشف عنها، الأمر الذي قد يسبب الضرر لمصالح المواطنين وقد يؤثر بشكل كبير في المؤسسات. حيث قدّرت تكلفة انتهاك بيانات الشركات بحوالي 3.92 مليون دولار (وفقاً لشركة IBM في 2019) .

وهذا التحدّي لن يختفي في الوقت القريب، فقد أُعلن عالمياً عن 3,800 انتهاك بيانات في الأشهر الست الأولى للعام 2019 حول العالم، باختراق حوالي 4.1 مليار ملف (حسب شركة الأمان المبني على المخاطر 2019).

وذلك يشكل تحدياً أمام الحكومات في كيفية إيجاد سياسة توازن بين تشجيع الابتكار وتحمي خصوصية الأفراد ضد أضرار انتهاك البيانات. علماً بأن أنظمة حماية البيانات الحالية تفرض معايير صارمة تُلزم المؤسسات على اتباعها في التعامل مع البيانات السرية والحساسة (مثل النظام الأوروبي العام لحماية البيانات، وقانون كاليفورنيا لخصوصية المتعاملين، وقانون مركز دبي المالي العالمي لحماية البيانات). هذه الأنظمة الحازمة المتخصصة بالمعلومات الشخصية تأتي على حساب توفير البيانات المفيدة وإتاحتها لتطبيقات تعلّم الآلة.

يتناول جهدنا هنا هذه التحديات بالتركيز على كيفية تعامل مؤسسات القطاع العام والخاص مع قضية التفاضل بين خصوصية ونفعية البيانات بشكل فعال.

تقنيات حماية الخصوصية التقليدية

توجد العديد من الطرق المستخدمة مسبقاً للحفاظ على معايير خصوصية البيانات، وكانت في معظمها تركز على تقنيات إخفاء الهوية من أجل تعديل أدوات تحديد الهوية (مركز خدمة البيانات، المملكة المتحدة، 2019)، ومن هذه التقنيات:

الحذف
وهي آلية حذف محدّدات الهوية من مجموعات البيانات (مثل شطب أو إبدال أسماء الأشخاص)

الاستبدال
وهي عملية إحلال أو استعاضة نقاط في البيانات الأصلية بقيم عشوائية (مثل استبدال الأسماء بمجموعة عشوائية من 16 خانة)

الإخفاء
وهي عملية تغطية حقل البيانات بحرف أو خانة مثل القناع (كالتغطية الجزئية لرقم البطاقة المكون من 16 رقماً بالرمز X مثل XXXX XXXX 2393 2480)

التجميع أو التعميم
وهي آلية تقوم بجمع البيانات في فئات عالية المستوى (مثل وضع سنة الميلاد بدلاً من تاريخ الولادة الكامل، أو فئات عمرية بدلاً من تحديد العمر برقم محدد)

تشمل هذه التكلفة جميع الأنشطة المتعلقة بالعمليات الأساسية التي تدفع مجموعة من النفقات المرتبطة باكتشاف خرق بيانات المؤسسات والاستجابة والاحتواء والمعالجة

وأثبتت تلك الآليات بأنها محدودة لحد ما حيث إن إخفاء هوية البيانات لغايات الخصوصية قد يحد من فاعلية ومرونة استخدام البيانات لغايات التحليل. وقد يكون لذلك أثراً عميقاً في بعض الأحيان. فتقنيات إخفاء الهوية فعالة بما يكفي لحماية خصوصية الأفراد في مجموعة البيانات، لكن ذلك يكون مقابل التخلّي عن الترابط بين خصائص البيانات، مما يحد من فرص التعرف على الأنماط التي تظهر لاحقاً في البيانات (دووك وروث، 2014، هاوي 2019، بايج، كابوت ونيسيم 2018).

يضاف إلى ذلك ما تناوله بحث جديد، يثبت أنه بتطبيق تقنيات حذف الهوية التقليدية على مجموعة بيانات مجهولة المصدر، يمكن لنماذج تعلم الآلة إعادة التعرف على الأفراد في عدد كبير من الحالات. وهكذا تضيع الخصوصية إلى جانب خسارة المنفعة من البيانات (روتشر، هندريكس، ومونجوي 2019).

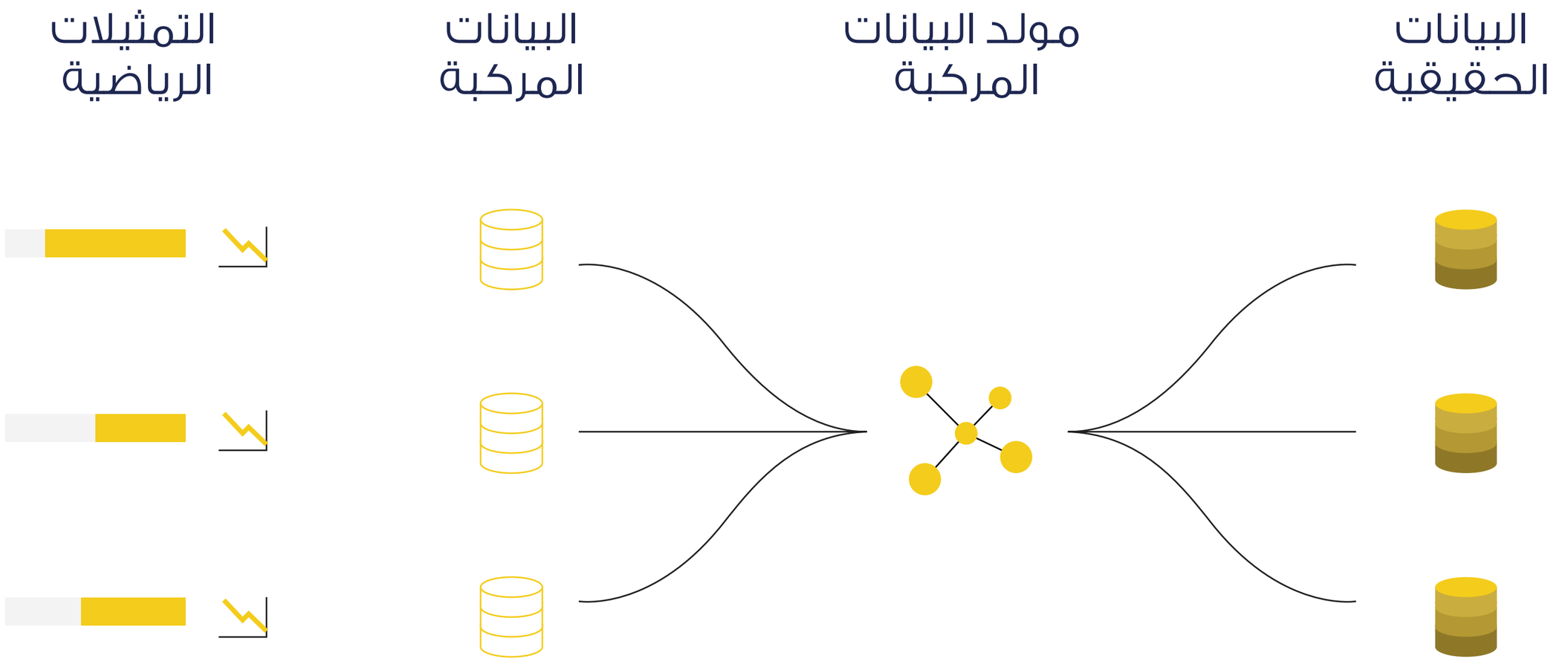
تطوير البيانات الاصطناعية

مكنت التطورات الحديثة من إنتاج في إنتاج البيانات الاصطناعية اصطناعياً أن تقدم بدائل متفوقة، فالتقنيات الحديثة للحقل الفرعي لتعلم الآلة ويعرف بـ(النماذج المنتجة generative modelling) يمكنها أن تساهم في إنتاج نسخ واقعية للغاية من البيانات لكنها مركّبة واصطناعية بالكامل من مجموعة بيانات حساسة أصلية.

النماذج المنتجة

تهدف (النماذج المنتجة generative modelling) إلى التعرف على التوزيع الحقيقي للبيانات لمجموعة تدريبية وذلك من أجل توليد نقاط بيانية جديدة مع بعض الاختلافات.

وتتفوق مجموعات البيانات الاصطناعية على الطرق التقليدية في مجال إخفاء الهوية من خلال الاحتفاظ بأنماط إحصائية أساسية في البيانات المرجعية، وذلك دون إعادة نسخ ملفات البيانات الأصلية (انظر الشكل 2.1).



الشكل 2.1: لمحة شاملة عن توليد البيانات الاصطناعية .

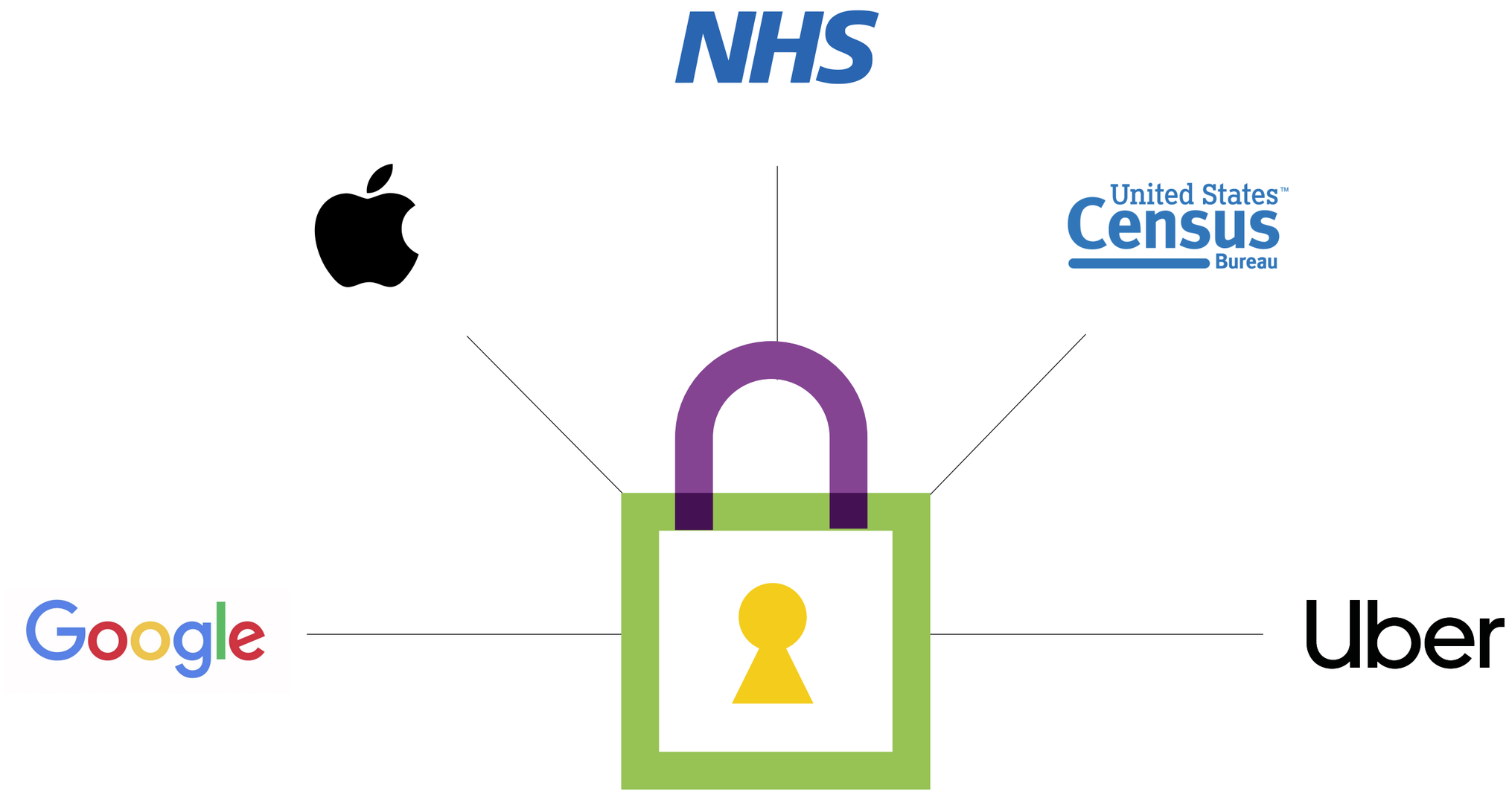
يجري خبراء خصوصية البيانات العديد من التجارب على البيانات الاصطناعية . وقد أظهر بحث أجراه المركز البريطاني للإحصاءات الوطنية أن هناك أنواع مختلفة من مجموعات البيانات الاصطناعية التي رفعت من القيمة المتولدة من تحليل البيانات مع حماية خصوصية الأفراد في مجموعات البيانات (بيتس، سباكولوفا، دوف وميلر، 2019).

القاعدة الذهبية: إنشاء البيانات الاصطناعية الخاصة باستخدام الخصوصية التفاضلية (differential privacy)

إن مفهوم الخصوصية التفاضلية يقوم على هذه التطورات، كما أنها تقدم إطار عمل رياضي متين للحد من الإفصاح الإحصائي ومخاطر إدارة الخصوصية، بينما تسمح في الوقت ذاته بمرونة عالية لمستخدمي البيانات (انظر الشكل 2.2). حيث إن تطبيق آلية الخصوصية التفاضلية يؤدي إلى توليد بيانات اصطناعية خاصة.

وتسمح الخصوصية التفاضلية للمستخدمين بتحديد درجة دقيقة من التحكم بالخصوصية والقابلية للاستخدام التي لم تستطع تحقيقها الطرق التقليدية، الأمر الذي يجعلها بديلاً مهماً وقاعدة ذهبية في حماية الخصوصية.

أما في مجال تعلم الآلة، فتضمن الخصوصية التفاضلية differential privacy) عدم استخدام أي فرد في مجموعة البيانات كعنصر معرّف أساسي في مخرجات عملية تعلم الآلة، وبذلك تحمي خصوصية الأفراد في مجموعات البيانات. وقد بدأ تبنيها فعلياً في مجالات أكاديمية ووكالات حكومية مثل مكتب التعداد الأمريكي في إجراء تعداد العام 2020، وعدد من الشركات التكنولوجية المرموقة (بايج، كابوت ونيسيم، 2018 وغارفنكل، 2018).



الخصوصية التفاضلية (differential privacy) حيز التطبيق

تتمتع نتائج **التعداد الأمريكي** بالحماية باستخدام الخصوصية التفاضلية، وقد تم استخدامها من أجل منع تتبع بيانات عدد معين من المتلقين.

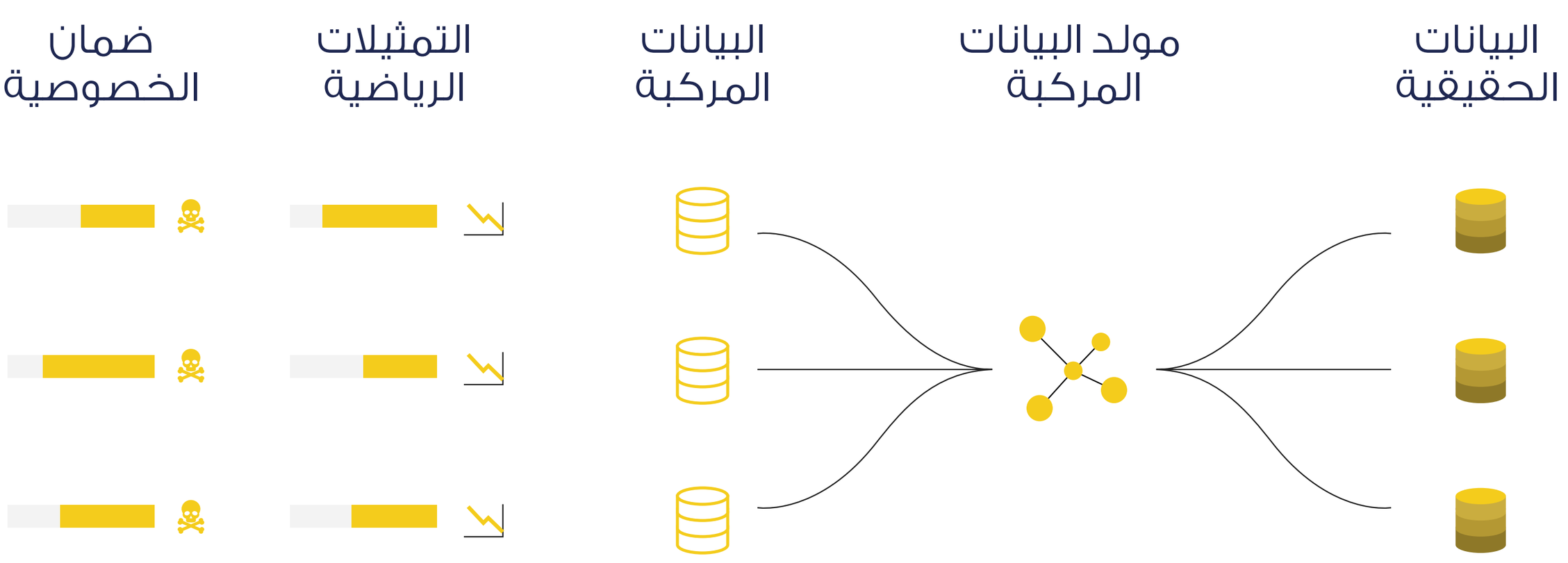
استخدمت **هيئة الخدمات الصحية الوطنية للمملكة المتحدة** (بالتحديد شبكة التصوير الإشعاعي في ميدلاند الشرقية)الخصوصية التفاضلية في إنشاء نسخ بيانات اصطناعية خاصة من بيانات مواعيد المرضى، ومكّنهم ذلك من إجراء التحليل الآمن من أجل تطوير الخدمة في المستقبل (مثل توقّع الطلب والقدرة الاستيعابية لخدمات سرطان الثدي).

تستخدم شركة "**آبل**" الخصوصية التفاضلية من أجل الحصول على تصوّر ما يقوم به المستخدمين مع الحفاظ التام على خصوصية الأفراد المستخدمين. وذلك يسمح للشركة بفهم أوساط المستخدمين دون الاطلاع على الأفراد ذاتهم في تلك الأوساط.

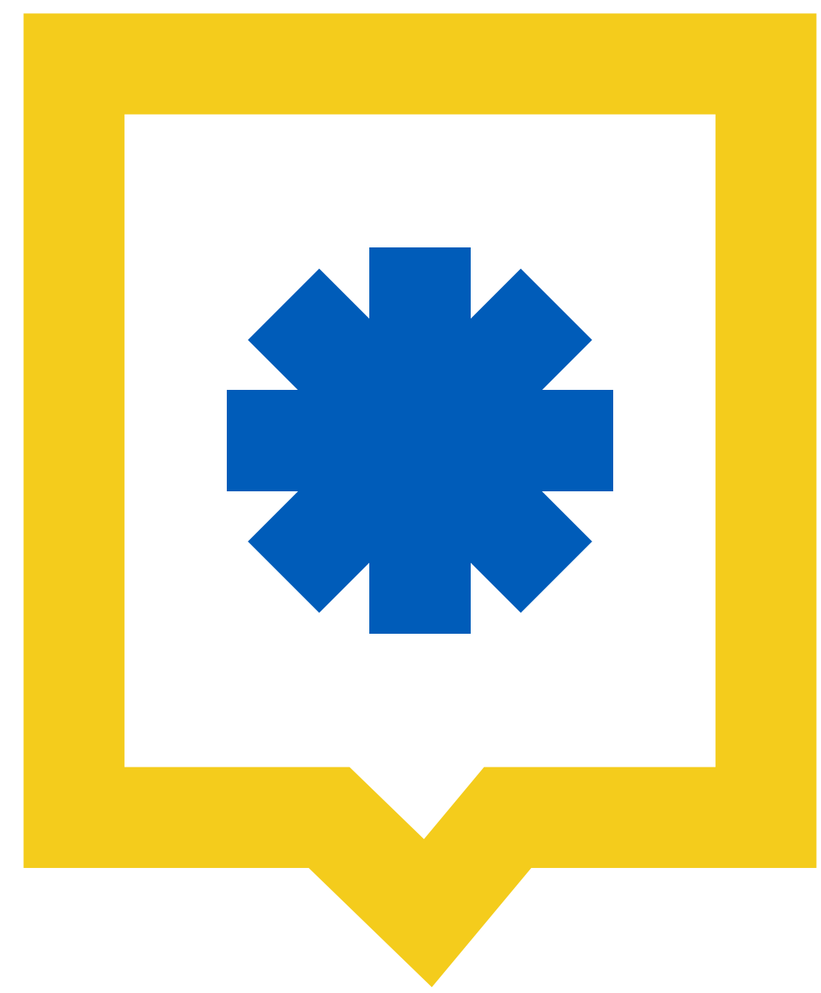
"**غوغل**" كانت قد استخدمت الخصوصية التفاضلية من أجل توفير تقارير انتقال كوفيد19– بشكل بيانات تجميعية مخفية الهوية تظهر حجم الإشغال لأنواع معينة من المواقع، وذلك لمنح مسؤولي القطاع الصحي معلومات تساعدهم في اتخاذ قرارات مصيرية في مواجهة كوفيد19–.

أطلق "**أوبر**" أداة مرجعية مفتوحة تتيح للشركات (ولشركة أوبر نفسها) جمع اتجاهات إحصائية عن المستخدمين مع الحفاظ على خصوصيتهم بنفس الوقت (باستخدام الخصوصية التفاضلية).

تسمح الخصوصية التفاضلية للمؤسسات العامة والخاصة بتطوير خدمات أفضل وأكثر ابتكاراً وتخصصاً لكل من المتعاملين والمواطنين. كما يمكنها أن تزود الحكومات بآلية تحمي خصوصية الأفراد من الأضرار الناشئة عن أي خروقات للبيانات مع تعزيز الابتكار القائم على البيانات في نفس الوقت.



الشكل 2.2: لمحة عامة لتوليد البيانات الاصطناعية الخاصة.



04

شرح تفصيلي غير تقني حول البحث ومخرجاته

شرح تفصيلي غير تقني حول البحث ومخرجاته

يتناول هذا الجزء:

الغاية من هذا البحث.

نقاش حول منهجية البحث والنتائج مع التركيز على تطبيق البيانات الاصطناعية الخاصة باستخدام الخصوصية التفاضلية (differential privacy) لمجموعات بيانات حوادث المرورعلى "دبي بالس."

مخرجات مبنية على نتائج البحث.

هذا الجزء مهم للقادة في القطاع الحكومي، وعلى خبراء علوم البيانات الانتقال إلى الجزء 5 و 6 للاطلاع على الشرح التقني للمواد والبحث والمخرجات.

الهدف

أردنا في هذا البحث قياس المنفعه من إنتاج مجموعات البيانات الاصطناعية الخاصة باستخدام الخصوصية التفاضلية - القاعد الذهبية الحالية في خصوصية البيانات - مع المحافظة على كل من السرية والنفعية (مرونة الاستخدام).

الهدف الأساسي هو إنتاج مجموعات لبيانات تحتفظ بأقصى درجة من مرونة الاستخدام مع المحافظة على الدرجة القصوى من الخصوصية. إلا أنه عند التطبيق نجد مفارقة بين هذين المبدأين ويظهر ذلك عند النظر إلى أمثلة لهما كنقيضين:

باستخدام مجموعة البيانات الحقيقية يمكن الانتفاع الكامل بها مقابل التنازل عن كامل الخصوصية (حيث تتألف البيانات من المعلومات الحساسة الأصلية وهو عامل فعال في النمذجة، لكنه يعني كذلك الإفشاء عن المعلومات الحساسة الخاصة بالأفراد).

في المقابل، إنشاء مجموعة بيانات اصطناعية من أرقام وحقول عشوائية يحافظ على كامل السرية على حساب مرونة الاستخدام (فالبيانات لن تحتوي على أي معلومات حساسة وأصلية، أي أن معلومات الأفراد الخاصة لن تنكشف، لكن لا يمكن تدريب نموذج تعلم الآلة باستخدام تلك البيانات كونها لا تحتوي على معلومات)

إن الغاية من هذا البحث

هي التحقق من مدى محافظة التقنيات المستخدمة على مرونة الاستخدام مع الحد من مخاطر الخصوصية لأكبر درجة ممكنة.

الهدف

لتجربة تلك التقنيات، استخدمنا 3 مجموعات بيانات لتدريب 3 نماذج مختلفة:

بيانات مركز UCI

حول البالغين من بيانات التعداد الأمريكي العام 1994. كان الهدف التنبؤ إذا ما كان سيتخطى دخل الفرد 50,000 دولار.

بيانات مركز UCI

حول نوع الغطاء من بيانات المسح الجيولوجي الأمريكي وكان الهدف توقع نوع نمو الغابات في منطقة معينة.

حوادث المرور في "دبي بالس"

مجموعة فرعية من بيانات مستخدمة في إنشاء أداة توقع لأسباب الحوادث

لغايات هذا الشرح غير التقني، سنقوم بالتركيز على النتائج المتعلقة بمجموعة بيانات حوادث المرور على منصة "دبي بالس".

وحتى يكون هذا البحث مرتبطاً بأرض الواقع، أجرينا مجموعة من التجارب بناء على 3 خيارات من آليات نشر البيانات، وهي مهمة لأي مالك بيانات وتمكنه من التعرف على قيمة ما لديه من البيانات مع حماية خصوصيتها. وهذه الخيارات هي:

1

إطلاق نموذج بيانات تم تدريبه بناءاً على بيانات خام وحساسة.

وفي هذه الحالة يكون هذا النموذج قياسياً وقادراً على التنبؤ بمتغيّر أو عمود معين من البيانات. (مثل إطلاق نموذج يصنف أسباب الحوادث المرورية)

قد يكون الفرد أو المؤسسة مهتمين بالخيار الأول عند إطلاق نموذج بيانات تم تدريبه وإتاحته للجمهور، مثلاً، إذا كان مزود الرعاية الصحية في دبي قد بنى نموذجاً يمكنه التنبؤ بما إذا أصيب مريضٌ ما بمرض معين، فقد يرغب بإتاحة ذلك النموذج لمزودي الرعاية الصحية الآخرين.

2

إطلاق نموذج يولد بيانات اصطناعية تم تدريبه على بيانات خام وحساسة

(مثل إطلاق نموذج ينتج بيانات اصطناعية عن البيانات الأصلية للحوادث المسجلة في الشرطة)

في حين يتعلق الخياران الثاني والثالث بحالة استخدام ترغب فيها المؤسسة بنشر بيانات اصطناعية على نطاق واسع لمؤسسات أخرى:

يمكن للمؤسسة عبر الخيار الثاني أن تولّد أي كمية مهما كانت كبيرة من البيانات الاصطناعية (كونها تملك حق الوصول لنموذج البيانات) إلى جانب الوصول إلى آليات عمل النموذج الذي يولّد البيانات الاصطناعية .

3

إطلاق بيانات اصطناعية تمثل البيانات الخام الحساسة

(مثل إطلاق نسخ مُركّبة اصطناعية عن بيانات حوادث المرور مباشرة للجمهور)

أما الخيار الثالث فيمنح المؤسسة قدراً محدداً وثابتاً من البيانات الاصطناعية (لأن المؤسسة لا تملك الوصول إلى النموذج الذي يولّد البيانات الاصطناعية).

ولتقييم مدى تأثير استخدام تقنيات الخصوصية التفاضلية في توليد البيانات الاصطناعية ، احتجنا لتناول كل من هذه الخيارات ومقارنتها مع آليات العمل الخاصة وغير الخاصة. وللقيام بذلك، قمنا بدايةً بتدريب نسخ خصوصية تفاضلية خاصة وغير خاصة للنموذج المتعلق بكل آلية إطلاق، وحاولنا تنفيذ هجمات للتعرف على مدى إمكانية الكشف عن المعلومات الخاصة. وقد اعتمدنا آلية "الهجوم الاستدلالي القائم على العضوية" أو ما يعرف بـ(membership inference attack) في تلك الهجمات، والتي تهدف إلى تحديد هوية الأفراد الذين كانوا جزءاً من دراسة أو تحليل.

النتائج

يوضح الشكل 3 نتائجنا لكل تجربة قمنا بها باستخدام مجموعة بيانات الحوادث المرورية على "دبي بالس"،

حيث ظهرت نتيجتين لكل آلية إطلاق: إحداها الفجوات في احتياطات حماية الخصوصية، والثانية استخدام الخصوصية التفاضلية في التدريب للمحافظة على خصوصية البيانات الأصلية.

	آلية الإطلاق	نوع التدريب	الخصوصية	النفعية (قابلية الاستخدام)
الخيار 1	مصنف مدرّب على بيانات خام (Classifier Trained)	غير خاص	52%	71%
		خاص	~100%	74%[2]
الخيار 2	نموذج توليدي مدرّب على بيانات خام	غير خاص	50%	72%
		خاص	98%	67%
الخيار 3	بيانات اصطناعية	غير خاص	90%	72%
		خاص	~100%	67%

الشكل 3: جدول نتائج التجارب على بيانات الحوادث المرورية من منصة "دبي بالس"

تثبت نتائجنا أن تدريب الخصوصية التفاضلية يدفع بنجاح كل آليات الإطلاق من هجمات الخصوصية دون التفريط بقابلية الاستخدام الأساسية.

قابلية الاستخدام

ارتبطت قابلية الاستخدام بدرجة دقة المصنف المدرّب، وفي الخيار الأول تم إطلاق المصنف، وللخيارين الثاني والثالث، المصنف كان نموذجاً جديداً مدرّباً على بيانات اصطناعية ناشئة من هذين الخيارين. وفي كل الحالات الثلاث، تم تقييم المصنف على بيانات حقيقية غير مكشوفة.

تسرب الخصوصية

أما تسرب الخصوصية فتم تحديده حسب ارتباطه بمعدل نجاح الهجمات المبنية على تعلم الآلة المصممة لتحري إذا ما كانت عينة الأفراد واردة في مجموعة البيانات الأصلية. مثل تلك الهجمة ستحقق دقةً بنسبة 50% بالتخمين العشوائي، وفي هذه الحالة يمكننا القول إن الخصوصية كانت 100%، وإذا كانت دقة الهجمة 100% يمكن القول بأن تسرب الخصوصية تبلغ 0%.

الاستنتاجات

يستنتج من البحث أن البيانات الاصطناعية الخاصة يجب الأخذ باعتبارها حلاً فاعلاً للمؤسسات في مواجهة التباين بين مبدأ الخصوصية ومرونة الاستخدام عند التعامل مع البيانات الحساسة. حيث يمكن لتلك التقنيات حماية المعلومات الحساسة المتعلقة بالأفراد عند إطلاقها مع الحصول على مرونة استخدام لمجموعة البيانات.

يضاف إلى ذلك أن القدرة على التحكم الدقيق بدرجات الخصوصية والاستفادة تعني أنه من الممكن التحكم بذلك التباين في ظروف معينة من حالات الاستخدام. لذلك من الطبيعي العمل على إنشاء نسخ مُركّبة خاصة من أي مجموعة بيانات حساسة يمكن استخدامها في عمليات التحليل وتعلم الآلة.

يحقق المعرف التفاضلي الخاص فائدة أكثر من نظيره غير الخاص. حدث هذا في هذا المثال بالذات لأن الخصوصية تمنع التجاوز ، إلى حد ما ، والمعرف الموضح هنا به زيادة في التجهيز. انظر الى القسم 6.2 لمعرفة السلوك الكامل كدالة لتركيب النموذج.

وصف التباين في مثال حي: وضعية مخاطر إعادة إدخال المريض

إذا افترضنا سيناريو نحاول فيه تأسيس مشروع لمعرفة إذا ما كان من الممكن بناء نموذج لاحتمالية إعادة الإدخال على مستوى المريض باستخدام السجلات الطبية. علماً بان السجلات الطبية تحتوي على معلومات سرية أو حساسة أو شخصية، لذلك فإن الضوابط المفروضة من إدارة المعلومات تكون شديدة.

وإذا ما استخدمت الخصوصية التفاضلية لإنشاء بيانات اصطناعية خاصة، يمكن حينها تطبيق درجات مختلفة من درجة الاستفادة وحماية الخصوصية حسب الطرف القائم بأعمال التحليل. مثلاً:

السيناريو الأول

فريق بيانات داخلي

إذا ما كان فريق بيانات داخلي يتولى مهمة التحليل، وبما أن البيانات لن تخرج من نظام الخادم المحلي، فقد يكون ملائماً رفع مستوى مرونة الاستخدام للحد الأعلى، ويمكن بنفس الوقت التحكم بمستوى الخصوصية بدقة لدرجة مقبولة من أجل تلبية متطلبات إدارة المعلومات.

السيناريو الثاني

فريق بيانات خارجي

إذا ما دعت الحاجة لإخراج البيانات من البيئة المحلية الآمنة ليتم تحليلها من قبل طرف ثالث، يجب رفع مستوى الخصوصية لأعلى حد - ذلك بسبب زيادة مخاطر وقوع السجلات الطبية في الأيدي الخاطئة.

باستخدام الخصوصية التفاضلية، يمكن التحكم كمّياً بدرجة حماية الخصوصية التي توفرها مجموعة البيانات الاصطناعية الخاصة، الأمر الذي يسمح لفريق إدارة المعلومات باتخاذ القرار الصحيح والمدروس قبل مشاركة البيانات مع الطرف الثالث. كما يمكن ضبط مدى مرونة الاستخدام للسماح بتقييم مدى نجاح المشروع المتوقّع.

كما نستنتج ما يلي:

تقنيات إخفاء هوية البيانات التقليدية لا تكفي دائماً للتعامل مع التباين بين معيارين أساسيين هما الخصوصية ومرونة الاستخدام. في معظم الحالات تكون قوية بما يكفي لحماية خصوصية الأفراد لكنها لا تكون مفيدة دائماً في مهام تحليل البيانات بشكل متكامل.

إطلاق أي نوع من النماذج للجمهور **بدون تدريب** متباين الخصوصية، **يكشف عن معلومات** الأفراد التي تعرّف عليها النموذج أثناء التدريب.

إذا ما تم تدريب النموذج باستخدام الخصوصية التفاضلية، ومن ثم تم **إطلاقه** للجمهور، فإن ذلك **لا يؤثر سلباً** على **خصوصية** البيانات أو **الاستفادة** من النموذج. لذلك يجب اتباع تلك الخطوة في جميع الحالات التي تم فيها تدريب النموذج على بيانات حساسة والمرغوب بإطلاقه.

دبـــــي الرقميـة

DIGITAL DUBAI

www.digitaldubai.ae