الذكاء الإصطناعي يقرأ أفكارك دون أن تشعر... تعرف على التفاصيل

طور باحثون في جامعات لندن ودورهام وساري نظامًا جديدًا "للذكاء الاصطناعي"، يمكنه التنصت على لوحة المفاتيح الخاصة بك لجمع البيانات التي يحتمل أن تكون حساسة.

وبحسب موقع "decrypt"، تم اختبار الخوارزمية، المقدمة في ورقة جديدة، على لوحة مفاتيح "MacBook Pro" وحققت دقة بنسبة 93-95٪ في اكتشاف المفاتيح التي تم الضغط عليها بناءً على التسجيلات الصوتية فقط.

ويوضح البحث أيضًا كيف توجد الميكروفونات في كل مكان في الهواتف وأجهزة الكمبيوتر المحمولة والأجهزة الأخرى، والتي يمكن بالتالي استخدامها لتهديد أمن البيانات من خلال هجمات القنوات الجانبية الصوتية.

بينما استكشفت الأوراق السابقة اكتشاف ضغطات مفاتيح الكمبيوتر المحمول عبر الصوت، فإن هذا النهج القائم على الذكاء الاصطناعي يحقق مستويات غير مسبوقة من الدقة.

ووفقًا للباحثين، فإن نموذج الذكاء الاصطناعي الخاص بهم يتجاوز أيضًا الأساليب الأخرى القائمة على الأجهزة، والتي تواجه قيود المسافة وعرض النطاق الترددي. ومع وجود الميكروفونات المضمنة في الأجهزة الاستهلاكية الشائعة، أصبحت صوتيات الكتابة أكثر تعرضًا للاختراق، ويمكن الوصول إليها من أي وقت مضى.

كيف تعمل خوارزمية الصوت الجديدة هذه؟
سجل الباحثون أولاً عينات صوتية من الكتابة على جهاز Pro MacBook، بالضغط على كل مفتاح 25 مرة.

وسمح ذلك لنظام الذكاء الاصطناعي بتحليل الاختلافات الدقيقة بين الصوت المنبعث من كل مفتاح.

تم تحويل التسجيلات الصوتية بعد ذلك إلى مخططات طيفية، وهي تمثيلات مرئية للترددات الصوتية بمرور الوقت.

كما تم تدريب نموذج الذكاء الاصطناعي على هذه المخططات الطيفية، وتعلم كيفية ربط الأنماط المختلفة بضربات المفاتيح المختلفة.

من خلال تطبيق عملية التدريب هذه عبر آلاف مقاطع الصوت، تتعرف الخوارزمية على الفروق الدقيقة بين البصمات الصوتية لكل مفتاح يتم الضغط عليه.

وبمجرد التدريب على لوحة مفاتيح معينة، يمكن للذكاء الاصطناعي تحليل التسجيلات الصوتية الجديدة والتنبؤ بضغطات المفاتيح بدقة عالية.

فيما وجد الباحثون أنه عند تدريب الخوارزمية على لوحة مفاتيح Pro MacBook، حققت دقة تتراوح بين 93-95٪. انخفض الأداء قليلاً فقط عند اختباره على أصوات لوحة المفاتيح في تسجيلات مكالمات Zoom.

ومع ذلك، يمكن أن يكون هذا النهج قابلاً للتطبيق على نطاق واسع إذا تمكن المهاجمون من الحصول على بيانات التدريب المناسبة.

وباستخدام نموذج مخصص، يمكن للجهات المختلفة أن تتعرف فيما بعد على كلمات المرور والرسائل ورسائل

البريد الإلكتروني والمزيد.

كيف تحمي نفسك؟

ومع استمرار الذكاء الاصطناعي في إطلاق العنان لإمكانيات جديدة لتسخير مصادر البيانات في كل مكان، سيتطلب الحفاظ على أمن البيانات والخصوصية براعة متساوية لتحديد نقاط الضعف غير المقصودة والتخفيف منها.