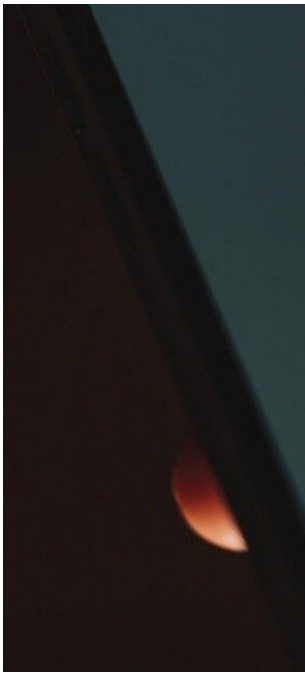
تقنية جديدة من ميتا تضمن تفاعلا آمنا مع الذكاء الاصطناعي عبر واتساب



تعمل "ميتا" على تقنية جديدة تُسمى المعالجة الخاصة لتطبيق واتساب، والتي تتيح للمستخدمين الوصول إلى أدوات الذكاء الاصطناعي فى بيئة خاصة وآمنة.

وقد شاركت ميتا ، لمحة أولى عن هذه التقنية وكيف تضمن أمان البيانات وشفافيتها على مستوى المستخدم، والجدير بالذكر أن الشركة تزعم أن الرسائل التي تتم مشاركتها مع الذكاء الاصطناعي والردود المُولّدة داخل هذه البيئة السحابية لا يمكن لأي شخص (بما في ذلك ميتا وواتساب) الوصول إليها باستثناء المستخدم وأي شخص آخر يتحدث إليه.

وتقول ميتا إن:"مستخدمي واتساب يمكنهم الوصول إلى ميزات الذكاء الاصطناعي دون المساس بالخصوصية، وشرحت الشركة بالتفصيل الرؤية الكامنة وراء المعالجة الخاصة والبنية التحتية متعددة الطبقات التي سيتم استخدامها لإنشاء هذه البيئة الآمنة".

وقد أعلنت الشركة أنها:"ستنشر قريبًا تفاصيل بعض المكونات التي استُخدمت في بناء هذه التقنية

لتمكين البحث المستقل في هذا المجال، حيث تهدف المعالجة الخاصة إلى تمكين المستخدمين من التفاعل مع الذكاء الاصطناعي من Meta واستخدام ميزات، مثل تلخيص الدردشات غير المقروءة وتوليد اقتراحات الكتابة، دون المساس بخصوصيتهم".

وكما يحل هذا المشكلة المتمثلة في دمج الذكاء الاصطناعي في WhatsApp دون إثارة مخاوف المستخدمين بشأن تخزين Meta لبياناتهم على خوادمها وخرق تشفير المنصة الشامل للرسائل والميزات الأخرى.

وصرحت ميتا بأنها، تُنشئ المعالجة الخاصة على بنية تحتية لبيئة تنفيذ موثوقة (TEE)، وهي جزء آمن من السحابة يُعالج البيانات دون الكشف عنها لأي شخص آخر.

وعلى سبيل المثال، إذا أرسل مستخدم طلبًا إلى الذكاء الاصطناعي لتلخيص رسائل مجموعة، فلن يتمكن من الوصول إلى هذه البيانات سوى جهاز المستخدم وبيئة المعالجة الآمنة،بالإضافة إلى ذلك، بمجرد معالجة التلخيص، تُحذف المعلومات من الخوادم.

وفيما يتعلق بالتفاصيل التقنية، ذكرت ميتا أن:"المعالجة الخاصة تستخدم تقنيات تشفير متقدمة مثل Oblivious HTTP وRemote Attestation لضمان إخفاء هوية المستخدم وبياناته ،حيث يتم توجيه كل طلب عبر مُرحِّلات خارجية، ويتم التحقق منه باستخدام السجلات العامة لضمان استخدام الكود المُعتمد فقط".

وتعني هذه المعالجة السرية أيضًا أنه لا يمكن لميتا ولا واتساب الوصول إلى البيانات المُدخلة إلى بيئة السحابة، سواءً أثناء نقلها إلى المعالجة الخاصة أو أثناء معالجتها، وفقًا للشركة.