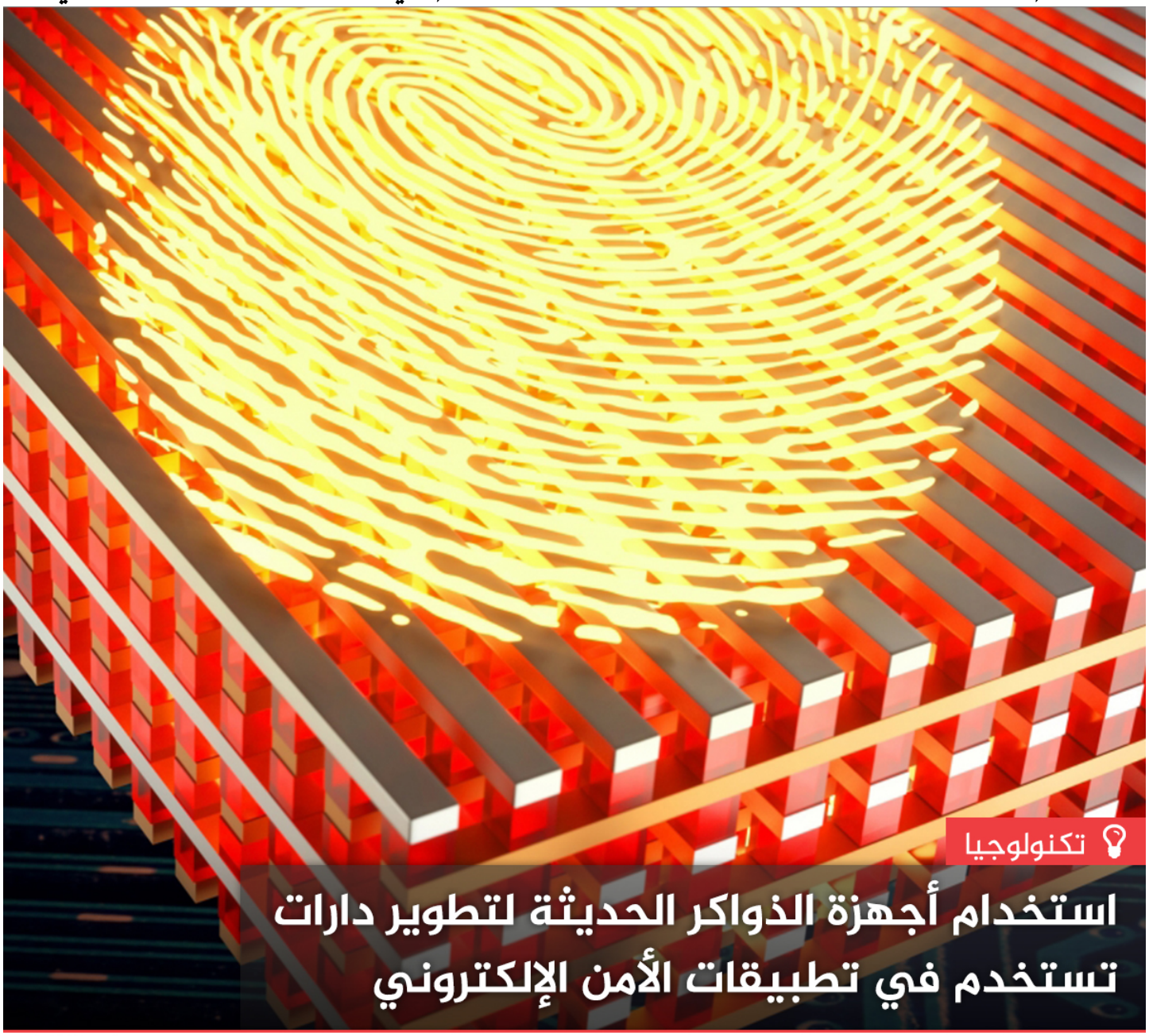
استخدام أجهزة الذواكر الحديثة لتطوير دارات تستخدم في تطبيقات الأمن الإلكتروني



رسم توضيحي للميمرستور كجهاز أمن إلكتروني ظهر على غلاف مجلة Nature Electronics. حقوق الصورة: Brian Long.

في حين أننا نتقبل دور تكنولوجيا إنترنت الأشياء **Internet of Things** في جعل حياتنا أكثر سهولة وانسيابية وراحة، إلا أن مخاطر الأمن الإلكتروني الناتجة عن ملايين الأجهزة والأدوات والآلات المتصلة مع بعضها لاسلكيًا لا تزال تشكل مصدر قلق كبير، حتى الهجمات المتفردة والموجهة قد تؤدي إلى أضرار شديدة، حيث أن خطر تدمير شبكة ما يتزايد عندما يتمكن المجرمون الإلكترونيون من التحكم والتلاعب بعدة عقد منها.

يعمل البروفيسور في علوم الحاسوب دميتري ستروكوف **Dmitri Stukov** من جامعة كاليفورنيا في سانتا باربرا **UC Santa Barbra**

على إيجاد حل لهذه المشكلة، حيث يبحث مع فريقه إمكانية إضافة طبقة إضافية من الحماية على الأجهزة التي تعمل بالإنترنت (والبلوتوث) والتي يتزايد عددها باستمرار، وذلك بالاعتماد على تكنولوجيا تهدف إلى منع الاستنساخ، وهي العملية التي تُنسَخ فيها العقد الموجودة في الشبكة ومن ثم تُستخدم لشن الهجمات من داخل الشبكة، إذ اقترح الفريق لعلاج هذه المشكلة الرقمية حلًا معتمدًا على جهاز ذاكرة تناظري وهو عبارة عن شريحة تحمل ما يُسمى بالميمريستور **Memristor** الأيوني.

يقول ستروكوف الذي نشر بحثه الجديد بعنوان "تفعيل أساسيات الأمن القائم على العتاد المادي بالاعتماد على الحالة التماثلية ومتغيرات التوصيل اللاخطية في أجهزة الميمرستور المضمنة" في مجلة **Nature Electronics**، يقول: "يمكنكم أن تعتبروها كالصندوق الأسود"، فبفضل طبيعتها تُعتبر الشريحة غير قابلة للاستنساخ فيزيائيًا، وبالتالي يصبح الجهاز محميًا من عمليات السرقة والتزييف والنسخ التي يقوم بها المجرمون الإلكترونيون.

أساس هذه التكنولوجيا هو الميمرستور، أو المقاومة الذاكرية، وهو عبارة عن مفتاح مقاومة كهربائية يمكنه "تذكر" حالة المقاومة الخاصة به بالاعتماد على تاريخ (القيم السابقة) التيار والجهود الكهربائية التي قام بتطبيقها، حيث أنه يقوم بتغيير خرجه استجابةً لهذه القيم السابقة.

بالإضافة إلى ذلك، وبسبب التركيب الفيزيائي للمادة المصنوعة منها الميمرستورات، فإن كل ميمرستور يكون متفردًا في استجابته للتيار والجهد المطبقَين، وبالتالي فإن الدارة المصنوعة من الميمرستورات تصبح كالصندوق الأسود، كما دعاها ستروكوف، ويكون من الصعب جدًا التنبؤ بقيم الخرج الخاصة بها اعتمادًا على قيم الدخل.

يقول ستروكوف: "تكمن الفكرة في أنه يصعب التنبؤ بعملها، وبسبب ذلك يصعب إعادة إنتاجها"، فإن المجال الواسع جدًا من قيم الدخل الممكنة ينتج عنه مجال مساوٍ (على الأقل) من قيم الخرج، وكلما زادت الميمرستورات المستخدمة زادت تلك الاحتمالات.
إن تجربة كل من الاحتمالات يستغرق وقتًا أكبر بكثير من الوقت الذي يمتلكه المهاجم منطقيًا لاستنساخ جهاز واحد، ناهيك عن شبكة كاملة من الأجهزة.

إن لاستخدام الميمرستورات في مجال الأمن الإلكتروني اليوم أهميةً كبيرة على ضوء الاختراق (التهكير) المعتمد على تعلم الآلة، وفيه تُدرَّب تكنولوجيا ذكاء اصطناعي على تعلّم ونمذجة قيم دخل وخرج مختلفة ومن ثم التنبؤ بالتسلسل التالي اعتمادًا على النموذج، إذ إنّه بفضل تعلم الآلة لا يحتاج المهاجم إلى أن يعرف ما الذي يحصل بالتحديد بينما يُدرَّب الحاسوب على مجموعة من مداخل ومخارج نظام ما.

يقول حسين نيلي **Hussein Nili** الكاتب الرئيس للبحث: "على سبيل المثال، إذا كان لديك مليونا قيمة خرج وتمكّن المهاجم من رؤية 10 آلاف أو 20 ألف قيمة منها، يصبح بإمكانه بالاعتماد عليها تدريب نموذج يمكنه محاكاة النظام فيما بعد".

يمكن للصندوق الأسود ذي الذاكرة الالتفاف على طريقة الهجوم هذه لأنه يجعل العلاقة بين المداخل والمخارج تبدو عشوائية أمام العالم الخارجي، بينما تحتفظ آليات العمل الداخلية للدارة بتكرارية كافية لتبقى موثوقة وفعالة، ويؤكد ذلك بقوله: "عليها أن تبدو عشوائية، ولكن عليها أن تكون حتمية أيضًا".

بالإضافة إلى قابلية التغير المضمنة في دارات الميمرستور هذه، هناك ميزات إضافية كالإنتاجية، والسرعة، والاقتصاد في استخدام الطاقة، والتي تجعلها مُكوِّنًا مثاليًا في تكنولوجيا إنترنت الأشياء التي تعمل بمخزون صغير من الطاقة.

أصبحت الميمرستورات بالفعل تكنولوجيا شبه عملية يمكن استخدامها لتأمين هوية الجهاز وكذلك تشفير المعلومات. يقول ستروكوف: "إذا تمكنا من التحكم بحجمها أكثر بقليل، قد تصبح العتاد المادي الأكثر تطورًا على العديد من المقاييس".

مع استمرار ستروكوف وفريقه في صقل هذه التكنولوجيا، فهم يبحثون في احتمال ظهور تغيرات في صفاتها مع الزمن، ويطورون أيضًا طرقًا أمنية قوية تتطلب دارات ميمرستور أكبر وتقنيات إضافية (مناسبة للمعدات العسكرية الحساسة أو المعلومات شديدة السرية)، وكذلك طرقًا ضعيفة موجهة نحو الإلكترونيات الاستهلاكية والأدوات اليومية، أي الأجهزة التي يكون من غير المرجح أن يقضي المهاجم ساعات أو أيام لمحاولة اختراقها.

- التاريخ: 2018-09-23
- التصنيف: تكنولوجيا

#تكنولوجيا #الذكاء الاصطناعي #علوم الحاسوب #إنترنت الأشياء

المصطلحات

- **الممرستور (Memristor)**: الممرستور أو الذاكرة المقاومة (Memristor) هو عنصر له طرفان تتغير مقاومته مع تغير الجهد، ولكن عندما ينقطع التيار تظل المقاومة كما هي، وهذا ما يعطي للعنصر صفة الذاكرة لأنها تحتفظ بآخر قيمة للمقاومة حتى بعد انقطاع التيار. وهذا يجعل الممرستور يناظر الوصلة العصبية بعقل الإنسان.

المصادر

- techxplore

المساهمون

- ترجمة
  - فرح درويش
- مُراجعة
  - حنان مشقوق
- تحرير
  - أحمد كنينة
  - رأفت فياض
- تصميم
  - عمرو سليمان
- صوت
  - ابتسام الخيال

- نشر
  - يقين الدبعي