

دراسات نقدية ٣ – الأسبوع الثامن

تقرير نقدي حول المهمة الثامنة: (نقد النظريات العلمية)
لورقة بحثية في مجال التخصص
"تقنية المعلومات"

إعداد الطالب/
عبد السلام العتيبي

٢٠٢٥م



بيانات الدراسة (موضع النقد)

البيانات	المحتوى	ترجمة المحتوى للعربية
عنوان الدراسة	Impact of AI on cybersecurity and security compliance	تأثير الذكاء الاصطناعي على الأمن السيبراني والامتثال الأمني
اسم المؤلف	Adebola Folorunso, Temitope Adewumi, Adeola Adewa, Roy Okonkwo and Tayo Nathaniel Olawumi	أديبولا فولورونسو، تيميتوبي أديومي، أديولا أديوا، روي أوكونكو، وتايو ناثانييل أولاومي
سنة النشر	٢٠٢٤	٢٠٢٤
جهة النشر	Global Journal of Engineering and Technology Advances	المجلة العالمية للتقدم في الهندسة والتكنولوجيا
رابط النشر	https://doi.org/10.30574/gjeta.2024.21.1.0193	https://doi.org/10.30574/gjeta.2024.21.1.0193

مقدمة

في إطار متطلبات مقرر "دراسات نقدية ٣"، يهدف هذا التقرير إلى تقديم نقد أكاديمي موضوعي وشامل لورقة بحثية بعنوان: "Impact of AI on cybersecurity and security compliance" (تأثير الذكاء الاصطناعي على الأمن السيبراني والامتثال الأمني) المنشورة عام ٢٠٢٤. وسيتم التركيز في هذا النقد على الجوانب النظرية والعلمية التي تناولتها الدراسة، مع تسليط الضوء على جوانب القوة والضعف، وتقديم أمثلة توضيحية من متن الورقة البحثية نفسها. سيختتم التقرير بتقديم رؤية مستقبلية للتطوير بناءً على الملاحظات النقدية.

نقد النظريات العلمية التي تم تناولها في الدراسة

تعتبر هذه الدراسة مراجعة شاملة لتأثير الذكاء الاصطناعي على الأمن السيبراني والامتثال الأمني، وتستعرض تطبيقاته وفوائده وتحدياته. بالرغم من أن الدراسة لا تستند إلى نظرية علمية واحدة أو إطار نظري محدد بوضوح، إلا أنها تتناول مجموعة من المفاهيم والتقنيات الأساسية التي تشكل أسس تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني، مثل:

. مفهوم تعلم الآلة (Machine Learning): حيث توضح الدراسة كيف يمكن لخوارزميات تعلم الآلة أن "تتعلم" من البيانات السابقة لاكتشاف التهديدات الجديدة.

. مفهوم التعلم العميق (Deep Learning): الذي تقدمه الدراسة كنوع أكثر تطوراً من تعلم الآلة، وتوضح استخدامه في تحليل مجموعات البيانات المعقدة للكشف عن الهجمات.

. النماذج التنبؤية (Predictive Models): وتُشير الدراسة إلى كيفية استخدام هذه النماذج للتنبؤ بالتهديدات الأمنية المستقبلية بناءً على تحليل الأنماط الحالية.

جوانب الضعف في تناول الجوانب النظرية:

- غياب النقد النظري العميق: تفتقر الدراسة إلى النقد المنهجي للمفاهيم التي تتناولها. فهي تقدمها كحلول جاهزة أكثر من كونها موضوعًا للبحث والنقد. على سبيل المثال، عند الحديث عن "تعليم الآلة" (Machine Learning)، لا تقدم الدراسة تحليلًا مقارنًا مفصلاً بين أنواع التعلم المختلفة وكيف تؤثر الاختلافات النظرية بينهما على دقة اكتشاف أنواع معينة من التهديدات، بل تصف وظائفها ببساطة.
- التعامل مع التحديات النظرية بشكل سطحي: تستعرض الدراسة التحديات المرتبطة بالذكاء الاصطناعي، مثل "الذكاء الاصطناعي العدائي" (adversarial AI)، ومخاوف خصوصية البيانات، والشفافية في عمليات اتخاذ القرار. لكنها لا تقدم إطارًا نظريًا قويًا لمواجهة هذه التحديات. على سبيل المثال، عند مناقشة "الذكاء الاصطناعي العدائي"، تُعرّف الدراسة المفهوم ببساطة دون التعمق في الأسس النظرية التي يجب أن تُبنى عليها النماذج الدفاعية الجديدة لمقاومة هذا النوع من الهجمات.
- التركيز على الوصف بدل التحليل: تظهر الدراسة أقرب إلى ورقة مراجعة أدبيات (review article) تهدف إلى تجميع المعلومات ووصفها، وهو ما يحد من قدرتها على تقديم نقد نظري أصيل أو بناء أطروحة جديدة، حيث أن الهدف الأساسي هو التلخيص.

رؤية شاملة للتطوير المستقبلي

بناءً على الملاحظات النقدية السابقة، يمكن للبحث المستقبلي أن يركز على الجوانب التالية لتقديم إسهام أكاديمي أكثر عمقاً وقيمة:

بناء إطار نظري جديد: يجب على الدراسات المستقبلية أن تتجاوز مجرد وصف تطبيقات الذكاء الاصطناعي وأن تسعى لتقديم إطار نظري يفسر كيفية تفاعل الذكاء الاصطناعي مع المشكلات الأمنية المعقدة. على سبيل المثال، يمكن تطوير إطار عمل نظري جديد لفهم "صندوق الذكاء الاصطناعي الأسود" (AI black box) وكيف يمكن زيادة شفافيته وقابليته للتفسير، وهو ما لم تتناوله هذه الدراسة بشكل كافٍ.

التركيز على النقد المنهجي: بدلاً من الاكتفاء بالوصف، يمكن للباحثين إجراء نقد منهجي للنماذج القائمة. على سبيل المثال، يمكنهم تحليل أداء النماذج المختلفة (مثل التعلم العميق مقابل تعلم الآلة الكلاسيكي) في سيناريوهات هجومية محددة، والبحث عن نقاط ضعف نظرية في كل نموذج.

دراسة الجوانب الأخلاقية والقانونية بعمق: يجب أن تتعمق الدراسات المستقبلية في الآثار الأخلاقية والقانونية لاستخدام الذكاء الاصطناعي، خاصة فيما يتعلق بخصوصية البيانات والتحيز. يمكن أن يركز البحث على تطوير مبادئ توجيهية نظرية لتطبيق الذكاء الاصطناعي بشكل عادل وشفاف، وهو ما يخدم أهداف برنامج الدكتوراه في التربية ومجال تقنيات التعليم، حيث تتداخل التحديات التقنية مع القضايا الإنسانية والاجتماعية.

خاتمة

تُعد هذه الدراسة مرجعاً مفيداً لفهم العلاقة بين الذكاء الاصطناعي والأمن السيبراني، فهي تقدم عرضاً شاملاً للمفاهيم الأساسية وتطبيقاتها العملية. ومع ذلك، فإن النقص في العمق النقدي والتحليلي للجوانب النظرية يُعد نقطة ضعف يجب الانتباه إليها. ولكي تساهم الدراسات المستقبلية في بناء معرفة أكاديمية راسخة، يجب أن تتبنى منهجية نقدية أعمق، وأن تعمل على بناء أطر نظرية جديدة، مع التركيز على الجوانب الأخلاقية والقانونية، بما يضمن تقديم إسهام حقيقي للمجال الأكاديمي والمهني.

المرجع

Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., & Olawumi, T. N. (2024). Impact of AI on cybersecurity and security compliance. Global Journal of Engineering and Technology Advances, 21(1),167-184.

<https://doi.org/10.30574/gjeta.2024.21.1.0193>



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

