

دراسات نقدية ١

الباحث/عبدالسلام العتيبي

محاضرة ١



دراسات نقدية ١

Enhancing Cybersecurity through AI and ML: Strategies,
Challenges, and Future Directions

إعداد
الباحث/عبدالسلام العتيبي

مقدمة عن الورقة العلمية :

في عصر تسود فيه التكنولوجيا الرقمية، أصبحت التهديدات السيبرانية تحديًا متزايدًا يواجه الأفراد والمؤسسات. مع تنوع أساليب الهجوم وتعقيدها، يتطلب الأمر استراتيجيات متقدمة لتأمين المعلومات وحماية الأنظمة. هنا تبرز أهمية الذكاء الاصطناعي وتعلم الآلة كأدوات فعالة لتحسين الأمن السيبراني، حيث توفر هذه التقنيات إمكانيات جديدة للكشف عن التهديدات والاستجابة لها بسرعة وفعالية.

معالجة كميات هائلة من البيانات في وقت قصير، مما يمكّن المؤسسات من اكتشاف ML و AI تتيح تقنيات الأنماط السلوكية المشبوهة والتنبؤ بالهجمات قبل وقوعها. ومع ذلك، تطرح هذه التقنيات أيضًا مجموعة من التحديات، بما في ذلك الحاجة إلى بيانات دقيقة وموثوقة، والتعقيدات التقنية في تطوير نماذج فعالة، بالإضافة إلى القضايا الأخلاقية المتعلقة بالخصوصية وحماية البيانات.

تهدف هذه الورقة العلمية إلى استكشاف استراتيجيات استخدام الذكاء الاصطناعي وتعلم الآلة في تعزيز الأمن السيبراني، مع التركيز على التحديات التي تواجه تنفيذ هذه التقنيات. كما تسعى الورقة إلى استشراف الاتجاهات المستقبلية في هذا المجال، مما يوفر إطارًا مفيدًا للممارسين والباحثين. من خلال تحليل الدراسات السابقة وجمع بيانات من خبراء في المجال، تسعى هذه الدراسة لتقديم رؤى قيمة تساهم في تطوير حلول أمنية أكثر فعالية لمواجهة التهديدات السيبرانية المتزايدة.

تسعى الورقة إلى تقديم مساهمة قيمة في المجال الأكاديمي والعملية، مما يساعد على تطوير حلول أكثر فعالية لمواجهة التهديدات السيبرانية المتزايدة حيث ركز على عدة اهداف منها :

استكشاف استراتيجيات الذكاء الاصطناعي في الأمن السيبراني: تحليل كيفية استخدام تقنيات الذكاء الاصطناعي وتعلم الآلة في تحسين كفاءة الأمن السيبراني، وتحديد الاستراتيجيات الأكثر فعالية.

[?] تحديد التحديات الرئيسية: تحديد التحديات التي تواجه تطبيق الذكاء الاصطناعي و ML في مجال الأمن السيبراني، بما في ذلك نقص البيانات، التعقيد الفني، والقضايا الأخلاقية.

تقييم فعالية النماذج المستخدمة: تقييم الأداء والفعالية لنماذج الذكاء الاصطناعي المختلفة في الكشف عن التهديدات السيبرانية والاستجابة لها.

استشراف الاتجاهات المستقبلية: استشراف الاتجاهات المستقبلية في استخدام الذكاء الاصطناعي في الأمن السيبراني، وكيف يمكن أن تؤثر التطورات التكنولوجية على هذا المجال.

تقديم توصيات عملية: تقديم توصيات مستندة إلى النتائج المستخلصة من البحث، لمساعدة المؤسسات في تحسين استراتيجياتها الأمنية من خلال تطبيق الذكاء الاصطناعي وتعلم الآلة.

تعزيز الفهم العام: تعزيز الفهم العام حول دور الذكاء الاصطناعي و ML في الأمن السيبراني، وتسلط الضوء على الفوائد والمخاطر المحتملة المرتبطة بها.



Thank You