

مقرر مهارات بحثية ١

الباحث/عبدالسلام العتيبي

محاضرة ١



مهارات بحثية ١

Machine Learning in Cybersecurity: Techniques and Challenges

إعداد
الباحث/عبدالسلام العتيبي

أهداف البحث:

١. تحليل تقنيات التعلم الآلي المستخدمة في الأمن السيبراني: دراسة الأدوات والخوارزميات المختلفة التي تُستخدم في الكشف عن التهديدات والتصدي لها.
٢. تقييم فعالية الأساليب المختلفة: مقارنة الأداء بين تقنيات التعلم الآلي التقليدية والحديثة في مواجهة التهديدات السيبرانية.
٣. تحديد التحديات والمشكلات: استكشاف التحديات الرئيسية التي تواجه تطبيق تقنيات التعلم الآلي في مجال الأمن السيبراني، مثل البيانات غير المتوازنة والتفسيرية.
٤. اقتراح حلول مبتكرة: تقديم أفكار وأساليب جديدة لتحسين فعالية تقنيات التعلم الآلي في الأمن السيبراني.
٥. توقع الاتجاهات المستقبلية: استشراف مستقبل تقنيات التعلم الآلي في مجال الأمن السيبراني وتوجهاتها.

أهمية البحث :

مواجهة التهديدات المتزايدة: يساعد البحث في توفير استراتيجيات فعالة للتصدي للتهديدات السيبرانية المتزايدة والمتطورة.

تحسين الأمن المعلوماتي: يساهم في تعزيز نظم الأمن السيبراني من خلال استخدام تقنيات متقدمة، مما يحسن الحماية ضد الهجمات.

توسيع المعرفة الأكاديمية: يضيف البحث إلى الأدبيات الأكاديمية حول دور التعلم الآلي في الأمن السيبراني، مما يعزز الفهم الأكاديمي والتطبيقي.

دعم المؤسسات: يوفر معلومات قيمة للمؤسسات حول كيفية استخدام التعلم الآلي بشكل أفضل لحماية أنظمتها وبياناتها.

تشجيع الابتكار: يحفز على البحث والابتكار في مجال الأمن السيبراني، مما يمكن أن يؤدي إلى تطوير حلول جديدة ومبتكرة.

المنهج العلمي الذي اعتمد عليه الباحث

- جمع المصادر: قام الباحث بتجميع مجموعة واسعة من المقالات الأكاديمية، والتقارير، والأوراق البحثية المتعلقة بتقنيات التعلم الآلي في الأمن السيبراني.
- تحليل المحتوى: تم تحليل الدراسات السابقة لفهم الأساليب المستخدمة، والنتائج المحققة، والتحديات التي واجهتها.

التجارب العملية:

- اختيار الخوارزميات: تم اختيار مجموعة من خوارزميات التعلم الآلي، مثل الشبكات العصبية، وآلات الدعم المتجهة (SVM)، وغابات القرار.
- إعداد البيانات: تم استخدام مجموعات بيانات معروفة في مجال الأمن السيبراني، مثل مجموعات بيانات الهجمات الإلكترونية، مع مراعاة تقسيم البيانات إلى تدريب واختبار.

- تنفيذ النماذج: جرى تنفيذ النماذج باستخدام بيئات برمجية مثل Python و R، مع استخدام مكتبات مثل Scikit-learn و TensorFlow.

التحليل الكمي:

- قياس الأداء: تم تقييم أداء النماذج باستخدام مؤشرات مثل الدقة، والحساسية، والخصوصية، ومعدل الخطأ.
- تحليل النتائج: تحليل البيانات الناتجة لتحديد أي الخوارزميات كانت الأكثر فعالية في الكشف عن التهديدات.

التحليل النوعي:

- دراسات الحالة: إجراء دراسات حالة على مؤسسات حقيقية استخدمت تقنيات التعلم الآلي، مع التركيز على كيفية تنفيذ الاستراتيجيات والمشاكل التي واجهتها.
- المقابلات: في بعض الحالات، يمكن إجراء مقابلات مع خبراء في الأمن السيبراني لفهم تجاربهم الشخصية.

التقييم والتفسير:

- تحليل النتائج: بعد جمع البيانات وتحليلها، تم تقييم النتائج بشكل شامل لتحديد فعالية التقنيات



Thank You