

تأثير تقنيات تعلم الآلة على تحسين الكشف عن الهجمات السيبرانية في شبكات الحاسوب

تحديد مجال المشكلة

- تُعد الهجمات السيبرانية من التحديات الكبرى التي تواجه شبكات الحاسوب الحديثة، وتلعب تقنيات تعلم الآلة دورًا متزايد الأهمية في تعزيز أنظمة الكشف عن هذه الهجمات. تهدف هذه الدراسة إلى مراجعة أحدث الأبحاث المتعلقة بكيفية استخدام تقنيات تعلم الآلة لتحسين الكشف عن الهجمات السيبرانية، مع تسليط الضوء على نقاط القوة والضعف في مختلف الخوارزميات والتقنيات مثل التعلم العميق، النماذج الهجينة، والتعلم التعزيزي.
- تشير الدراسات إلى فاعلية تقنيات تعلم الآلة والتعلم العميق في تحسين الكشف والتصنيف في أمن الشبكات، مع اختلاف تركيز كل دراسة بين الكشف المبكر، التصنيف، واختيار الخصائص. هناك توافق في أهمية تعزيز النماذج لمقاومة الهجمات العدائية، وتحديات في التعامل مع البيانات الحقيقية ومتطلبات الموارد.

وصف المشكلة

تُعد حماية شبكات الحاسوب من الهجمات السيبرانية من أبرز التحديات في مجال أمن المعلومات، حيث تتزايد وتتعقد أساليب الهجوم باستمرار

إبراز الأهمية

- رغم التطورات المتسارعة في تقنيات تعلم الآلة، لا تزال أنظمة الكشف عن الهجمات السيبرانية تواجه مشاكل عدة، مثل ضعف الكشف المبكر لبعض الهجمات المعقدة، ارتفاع معدلات الإنذارات الكاذبة، وقلة البيانات الحقيقية المستخدمة في تدريب النماذج. كما أن بعض النماذج، خاصة التي تعتمد على التعلم العميق، تحتاج إلى موارد حسابية ضخمة، مما يحد من تطبيقها في الوقت الحقيقي.
- تحسين دقة وكفاءة أنظمة الكشف عن الهجمات ضروري لحماية الشبكات من الاختراقات والخسائر المحتملة، كما أن تطوير نماذج مقاومة للهجمات العدائية هو أمر حيوي للحفاظ على أمن البيانات.

ذكر الحلول الحالية

تم اقتراح عدة حلول، منها خوارزميات **SVM** ، الشبكات العصبية العميقة، النماذج الهجينة التي تجمع بين **Neural Networks** و **Random Forest**، والتعلم التعزيزي في الوقت الحقيقي، إلا أن كل منها يعاني من تحديات خاصة مثل تعقيد النماذج، متطلبات الموارد، وقلة التكيف مع تهديدات متغيرة

تبرير الحاجة إلى البحث

لذلك، هناك حاجة ملحة لتطوير إطار عمل متكامل يجمع بين دقة الكشف، الكفاءة الحسابية، والقدرة على التكيف مع التهديدات الجديدة، مع التركيز على استخدام بيانات حقيقية وتحسين مقاومة الهجمات العدائية

الأهداف البحثية

- اقتراح إطار عمل متكامل باستخدام تقنيات تعلم الآلة لتحسين الكشف عن الهجمات السيبرانية في شبكات الحاسوب
- تصميم نماذج هجينة فعالة توازن بين دقة الكشف واستهلاك الموارد الحسابية
- تقييم أداء النماذج المقترحة باستخدام مجموعات بيانات حقيقية لضمان التطبيق العملي
- تطوير آليات لتعزيز مقاومة النماذج للهجمات العدائية
- تحليل تأثير تقنيات اختيار الخصائص على أداء وتعقيد النماذج

المراجع

كيف يمكن استخدام الذكاء الاصطناعي والتعلم الآلي في تعزيز الأمن السيبراني في السعودية؟

<https://www.rmg-sa.com/%D9%83%D9%8A%D9%81-%D9%8A%D9%85%D9%83%D9%86-%D8%A7%D8%B3%D8%AA%D8%AE%D8%AF%D8%A7%D9%85-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D9%88%D8%A7%D9%84/>

التعلم العميق في الذكاء الاصطناعي

<https://betraining.com.sa/ar/blog/%D8%A7%D9%84%D8%AA%D8%B9%D9%84%D9%85-%D8%A7%D9%84%D8%B9%D9%85%D9%8A%D9%82-%D9%81%D9%8A-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A>

تطبيقات الأمن السيبراني

<https://oercommons.org/courseware/lesson/113075/overview>

دراسة أنظمة كشف التسلل إلى الشبكات باستخدام الذكاء الاصطناعي/التعلم الآلي

<https://www.mdpi.com/2076-3417/12/22/11752>

الاسم: مصعب عبدالله السلامه

الرقم الأكاديمي: 252000152