

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

## مقدمة

تُعد الهجمات السيبرانية من التحديات الكبرى التي تواجه شبكات الحاسوب الحديثة. تلعب 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

## Machine Learning Approaches for Cybersecurity Intrusion Detection: A Survey

الأهداف: استعراض تقنيات تعلم الآلة المختلفة المستخدمة في الكشف عن التسلل

مقارنة بين خوارزميات التصنيف مثل

SVM

أظهرت نتائج جيدة في تحسين معدلات الكشف مع تقليل الإنذارات الكاذبة

نقاط القوة: تغطية شاملة للمنهجيات المختلفة

نقاط الضعف: قلة البيانات الحقيقية المستخدمة في بعض الدراسات

## Deep Learning-Based Network Anomaly Detection

الأهداف: استخدام التعلم العميق للكشف عن الشذوذ في حركة الشبكة

تطبيق شبكات

CNN و LSTM

على مجموعات بيانات متنوعة

النتائج: تحسين دقة الكشف بشكل ملحوظ مقارنة بالطرق التقليدية  
نقاط القوة: القدرة على معالجة بيانات ضخمة ومتنوعة  
مع العلم انه يحتاج الى موارد حسابية عالية

## Hybrid Machine Learning Model for Cyber Attack Classification

الأهداف: دمج خوارزميات متعددة لتحسين تصنيف الهجمات

استخدام نموذج هجين يجمع بين

Random Forest و Neural Networks

النتائج: تحسين دقة التصنيف وتقليل الأخطاء

نقاط القوة: الابتكار في دمج الخوارزميات

نقاط الضعف: زيادة تعقيد النموذج مما يؤثر على الأداء

## Real-Time Intrusion Detection Using Reinforcement Learning

الأهداف: تطوير نظام كشف تسلل في الوقت الحقيقي باستخدام التعلم التعزيزي

الطرق: تطبيق خوارزميات

Q-learning

على بيانات الشبكة

نظام قادر على التكيف مع التهديدات المتغيرة

نقاط القوة: العمل في الوقت الحقيقي والتكيف الذاتي

نقاط الضعف: متطلبات عالية للمعالجة

## Feature Selection Techniques for Network Security

الأهداف: تحسين أداء نماذج التعلم الآلي باختيار الخصائص المناسبة

مقارنة طرق اختيار الخصائص وتأثيرها على دقة النماذج

النتائج: تحسين الكفاءة وتقليل التعقيد دون فقدان دقة كبيرة

نقاط القوة: زيادة فعالية النماذج

نقاط الضعف: خطر فقدان معلومات مهمة أثناء الاختيار

## Adversarial Machine Learning Attacks in Cybersecurity

الأهداف: دراسة الهجمات العدائية وتأثيرها على نماذج التعلم الآلي

تحليل استراتيجيات الهجوم وتقنيات الدفاع

النتائج: الحاجة إلى تطوير نماذج مقاومة للهجمات

نقاط القوة: تسليط الضوء على تحديات جديدة

نقاط الضعف: الأبحاث لا تزال في مراحلها المبكرة

## التحليل

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

## خاتمة

تؤكد مراجعة الأدبيات أهمية تقنيات تعلم الآلة والتعلم العميق في تعزيز أمن الشبكات، مع التركيز على التحديات المتعلقة بالبيانات الحقيقية والموارد. ينبغي توجيه الأبحاث المستقبلية لتطوير نماذج أكثر كفاءة وقادرة على مقاومة الهجمات العدائية

الاسم: مصعب عبدالله السلامه

الرقم الأكاديمي: 252000152