وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم البرمجيات

تطبيق خوارزميات التعلم الألي على البرمجيات الخبيثة

رسالة مقدمة
إلى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
وهي جزء من متطلبات نيل شهادة ماجستير علوم في
البرمجيات

الطالبة
ناز فاتح محمد جميل محمود

بإشراف
م .د. منى محمد طاهرجوهر

١٤٤٥ هـ ٢٠٢٤ م

المستخلص

مع تزايد الاعتماد على الأجهزة الذكية، تطورت التهديدات الإلكترونية، مما جعل البرمجيات الضارة تشكل خطراً متزايداً على خصوصية وأمن المستخدمين. تتميز هذه البرمجيات الخبيثة بنقل البيانات بشكل غير منتظم، مما يجعلها من بين أكثر الهجمات الإلكترونية شيوعاً وتزايداً على الإنترنت. نظراً لتعقيد وتنوع هذه الهجمات، أصبح من الضروري تطوير أساليب دفاعية متقدمة، حيث يلعب الأمن السيبراني وتقنيات التعلم العميق، المستمدة من الأبحاث النظرية، دوراً مهماً كبديل عن الأساليب التقليدية لمواجهة هذه التهديدات

توفر تقنيات التعلم العميق أدوات فعالة للتعرف والتصنيف الدقيق للبرمجيات الضارة، مما يعد حاسماً في مواجهة التحديات الأمنية المعاصرة. على الرغم من استمرار التحديات المتعلقة بمعالجة البيانات الضخمة والمعقدة، فقد أثبتت أساليب الذكاء الاصطناعي والتعلم العميق تفوقها في دقة وكفاءة كشف البرمجيات الضارة مقارنة بالطرق التقليدية. هذا يدفع الباحثين في مجال الأمن السيبراني نحو تحسين وتطوير هذه التقنيات المتقدمة. في هذه الرسالة، تم تقديم نموذجاً جديداً للكشف عن البرامج الضارة يستخدم مزيجاً من خوارزميات التعلم العميق والتعلم الآلي، مثل الشبكات العصبية متعددة الطبقات(MLP) ، الشبكات العصبية المتكررة،(RNN) ،الذاكرة طويلة الأمد(LSTM) ، وخوارزمية الغابة العشوائية. (RF) ،تم تطبيق هذه الخوارزميات على مجموعة بيانات Ember تشمل مقاييس أداء مثل الدقةF١درجة،الاستدعاء،الضبط لتقييم فعاليتها.

أظهرت النتائج أن دمج الشبكات العصبية متعددة الطبقات مع خوارزمية الغابة العشوائية يعطي أفضل أداء في الكشف عن البرمجيات الضارة، بدقة وصلت إلى ٩١%. هذه النتائج تؤكد على الإمكانيات الهائلة التي يقدمها التعلم العميق لتعزيز الأمن السيبراني.

Ministry of hi Higher Education and

Scientific Research

University Of Mosul

College Of Computer Sciences and

Mathematics

Department of Software

Applying machine learning algorithms to malware

A Thesis Submitted to the Council of the College of Computer Science and Mathematics

University of Mosul

as a Partial Fulfillment of Requirements for the Degree of Master of Science

in

Software

Naz Fatih Mohamed jamee

Supervised By

Dr. Muna Mohamed Tahir

20224 A. D **1445 A. H**

Abstract

With increasing reliance on smart devices, cyber threats have evolved, making malware an increasing threat to users' privacy and security. This malware is characterized by irregular data transmission, making it among the most common and growing cyber-attacks on the Internet. Due to the complexity and diversity of these attacks, it has become necessary to develop advanced defensive methods, as cyber security and deep learning techniques, derived from theoretical research, play an important role as an alternative to traditional methods to confront these threats.

Deep learning techniques provide powerful tools for accurate identification and classification of malware, which is crucial to addressing contemporary security challenges. Although challenges related to processing large and complex data remain, artificial intelligence and deep learning methods have proven superior in the accuracy and efficiency of malware detection compared to traditional methods. This drives research in the field of cyber security towards improving and developing these advanced technologies. In this thesis, a new malware detection model is presented that uses a combination of deep learning and machine learning algorithms, such as multi-layer neural networks, recurrent neural networks, long-term memory, and random forest algorithm. These algorithms were applied to a dataset that includes performance metrics such as precision, recall, precision, and F١ to evaluate their effectiveness and rate

The results showed that combining multi-layer neural networks with the random forest algorithm provides the best performance in detecting malware, with an accuracy of ٩١٪. These results underscore the enormous potential that deep learning offers to enhance cyber security