

اكتشاف البرمجيات الضارة في الحوسبة السحابية باستخدام تحسين اختيار المعدلة White Shark الميزات في خوارزمية

إعداد

محمد حمدان الزيود

إشراف

الدكتور حسام مصطفى

الملخص

أدت التطورات في تكنولوجيا المعلومات إلى انتشار الحوسبة السحابية ، والتي أصبحت ومع ذلك ، تظل سلامة البيانات . الآن البديل المفضل لمعظم مؤسسات تكنولوجيا المعلومات مصدر قلق كبير بسبب البنية التحتية المفتوحة والشاملة للحوسبة السحابية ، مما يجعلها لذلك ، أصبح ضمان أمان البيانات وسلامتها أولوية قصوى ، عرضة لهجمات القرصنة، كما أن تطوير نظام اكتشاف التسلسل غير الطبيعي باستخدام تقنيات التعلم الآلي يعد حلاً يتطلب التحدي المتمثل في العثور على . محتملاً لتحديد الهجمات السحابية المتكررة ومنعها أنظمة فعالة ومثالية للكشف عن التسلسل في الشبكة استخدام مجموعات بيانات التطفل المحدثة (مع خوارزمية تحسين KNN و (SVM) وتقنيات التعلم الآلي ، يتم دمج آلة متجه الدعم ، ليتم تقييم أداء الخوارزمية المقترحة باستخدام مقاييس الدقة والتذكر . (WSO) القرش الابيض مع نتائج الابحاث السابقة) KNN و (SVM) تمت مقارنة الخوارزمية المقترحة بناءً على (، والتي استخدمت Kyoto) و (NSL-KDD) الذي استخدمت نفس مجموعتين البيانات (جميعها للتنبؤ باكتشاف التسلسل غير الطبيعي ، أظهرت النتائج أفضل دقة عند 99.8% عند استخدام خوارزمية تحسين القرش الابيض واستخدام مجموعتين البيانات ، وكانت النتيجة متساوية تقريباً عند استخدام خوارزمية تحسين القرش الأبيض المعدلة بدقة 99.9% من مجموعتين البيانات الخاصه بالتنبؤ عن اكتشاف التسلسل غير الطبيعي.

**Malware Detection in Cloud Computing Using Feature
Selection Based on Modified White Shark Algorithm
(WSO) Optimization**

Prepared by

Mohammad Hamdan Al-Zyod

Supervision by

Dr. Hossam Mustafa

Abstract

Advances in information technology have led to the spread of cloud computing, which is now the preferred alternative for most IT organizations. However, data safety remains a major concern due to the open and comprehensive infrastructure of cloud computing, which makes it vulnerable to hacker attacks. Therefore, ensuring data security and integrity has become a top priority, and developing an abnormal intrusion detection system using machine learning techniques is a potential solution to identify attacks. Recurrent clouding and prevention. The challenge of finding efficient and optimal network intrusion detection systems requires the use of updated intrusion datasets and machine learning techniques. Support vector machine (SVM) is integrated with White Shark Optimization

algorithm. Utilizing criteria for recall and accuracy, the suggested algorithm is judged for its effectiveness. The proposed algorithm based on (SVM) was compared with the results of the previous research that used the same two datasets (NSL-KDD) and (Kyoto), which were all used to predict the detection of abnormal infiltration, the results showed the best accuracy at 99.8% when using the white shark optimization algorithm. And using the two data sets, the result was almost equal when using the modified white shark optimization algorithm with an accuracy of 99.9% of the two data sets for predicting the detection of abnormal intrusion.

Keywords: Malware detection; Machine learning; White Shark Algorithm; Cloud computing.

