An Intelligent Crypto-Locker Ransomware Detection Technique Using Support Vector Machine Classification and Grey Wolf Optimization Algorithms

Abdullahi Mohammed Maigida, Shafi'i Muhammad Abdulhamid, Morufu Olalere, Idris Ismaila

Abstract

Ransomware is advanced malicious software which comes in different forms, with the intention to attack and take control of basic infrastructures and computer systems. The majority of these threats are meant to extort money from their victims by asking for a ransom in exchange for decryption keys. Most of the techniques deployed to detect this could not completely prevent ransomware attacks because of its obfuscation techniques. In this research work, an intelligent crypto-locker ransomware detection technique using Support Vector Machine (SVM) and Grey Wolf Optimization (GWO) algorithm is proposed to overcome the malware obfuscation technique because of its ability to learn, train and fit dataset based on the observed features. The proposed technique has shown remarkable prospects in detecting cryptolocker ransomware attacks with high true positive and low false positive rate.
Keywords: Support Vector Machine, Grey Wolf Optimization, Ransomware, Crypto-locker, Malware.

https://www.proquest.com/openview/d1bf8c214e8a005e1cbfb04cadd69163/1?pq-origsite=gscholar&cbl=2030612