Malware analysis performance enhancement using cloud computing

ABSTRACT

Nowadays, computer based technology has taken a central role in every person life. Hence, damage caused by malicious software (malware) can reach and effect many people globally as what could be in the early days of computer. A close look at the current approaches of malware analysis shows that the respond time of reported malware to public users is slow. Hence, the users are unable to get prompt feedback when reporting suspicious files. Therefore, this paper aims at introducing a new approach to enhance malware analyzer performance. This approach utilizes cloud computing features and integrates it with malware analyzer. To evaluate the proposed approach, two systems had been prepared carefully with the same malware analyzer, one of them utilizes cloud computing and the other left without change. The evaluation results showed that the proposed approach is faster by 23 % after processing 3,000 samples. Furthermore, utilizing cloud computing can open door to crowd-source this service hence encouraging malware reporting and accelerate malware detection by engaging the public users at large. Ultimately this proposed system hopefully can reduce the time taken to detect new malware in the wild.

Keyword: Malware analysis; Cloud computing; Malware detection