Host Based Intrusion Detection and Prevention Model Against DDoS Attack in Cloud Computing

Aws Naser Jaber[1(✉)], Mohamad Fadli Zolkipli[1,2], Hasan Awni Shakir[2], and Mohammed R. Jassim[2,3]

[1] Faculty of Computer Systems and Software Engineering, Gambang, Malaysia
Naserjaber.a@gmail.com
[2] National University of Malaysia, Bangi, Malaysia
fadli@ump.edu.my, p86690@siswa.ukm.edu.my
[3] University of Technology, Baghdad, Iraq
mrj_1212@yahoo.com

Abstract. Cloud computing has become an innovative technology. Recent advances in hardware and software have put tremendous pressure on administrators, who manage these resources to provide an uninterrupted service. System administrators should be familiar with cloud-server monitoring and network tools. The main focus of the present research is the design of a model that prevents distributed denial-of-service attacks based on host-based intrusion detection protection systems over hypervisor environments. The prevention model uses principal component analysis and linear discriminant analysis with a hybrid, nature-inspired metaheuristic algorithm called Ant Lion optimisation for feature selection and artificial neural networks to classify and configure the cloud server. The current results represent a feasible outcome for a good intrusion detection and prevention framework for DDoS-cloud computing systems based on statistics and predicted techniques.