Challenges and opportunities for intrusion detection system in cloud computing environment

Hesham Mohamed Mostafa Mohamed Mahmoud Elmasry ,Ayman Elsayed Khedr, Ahmed Abd elkaderHatem

Abstract

The paper suggests an anomaly multi Phases intrusion detection technique for discovering the zero-day, fast-spreading and complicated network attacks on the cloud platform with the least amount of false alarm rate. Cloud computing is commonly regarded as an attractive business model, because it minimizes expenditure and its costs are directly related to use and demand. But the distributed nature of cloud computing environments, their vast aggregation of resources, large user access, efficient and automated resource sharing allow Intruders to use cloud to their advantage. The objective of this paper is to use the comparative approach to review, analyze and evaluate all of the existing Intrusion Detection Systems (IDSs) types, techniques, algorithms and all of the previous attempts related to securing and detecting the attacks on the cloud environment. The article concluded that the existing IDS techniques and algorithms are not capable in detecting the unknown attacks with minimum false alert rate in cloud platform. The effectiveness of the new intrusion detection technique can be evaluated by measuring the accuracy and false alert rate.

Journal of Theoretical and Applied Information Technology 2020, October