

Network Intrusion Detection Framework Based on Whale Swarm Algorithm and Artificial Neural Network in Cloud Computing

Ahmed Mohammed Fahad^(✉), Abdulghani Ali Ahmed,
and Mohd Nizam Mohmad Kahar

Faculty of Computer Systems & Software Engineering,
Universiti Malaysia Pahang, 26300 Kuantan, Malaysia
ahmedsipher2010@yahoo.com,
{abdulghani, mnizam}@ump.edu.my

Abstract. Cloud computing is a rapidly developing Internet technology for facilitating various services to consumers. This technology suggests a considerable potential to the public or to large companies, such as Amazon, Google, Microsoft and IBM. This technology is aimed at providing a flexible IT architecture which is accessible through the Internet for lightweight portability. However, many issues must be resolved before cloud computing can be accepted as a viable option to business computing. Cloud computing undergoes several challenges in security because it is prone to numerous attacks, such as flooding attacks which are the major problems in cloud computing and one of the serious threat to cloud computing originates came from denial of service. This research is aimed at exploring the mechanisms or models that can detect attacks. Intrusion detection system is a detection model for these attacks and is divided into two-type H-IDS and N-IDS. We focus on the N-IDS in Eucalyptus cloud computing to detect DDoS attacks, such as UDP and TCP, to evaluate the output dataset in MATLAB. Therefore, all technology reviews will be solely based on network traffic data. Furthermore, the H-IDS is disregarded in this work.

Keywords: IDS · WOA · ANN · TUIDS · Cloud computing