Managing Intrusion Detection as a Service in Cloud Networks

Abstract

Cloud computing is frequently being utilized to eliminate the need to local information resources. In this paper, we address the problem of intrusion detection in cloud environments and the possibility of allowing intrusion detection to be provided to clients as a service. The paper describes the Cloud Intrusion Detection Service (CIDS), which is intended to function as an intrusion detection web service to be provided for cloud clients in a service-based manner. CIDS utilizes the "Snort" open source intrusion detection system. The operating logic and user access webpages were developed using J2EE. We implemented a proof-of-concept prototype to evaluate the performance. CIDS was proved to be very friendly to resource allocation. Additionally, CIDS gave better attack detection rates and attack detection times than other solutions. These improvements can be beneficial to both cloud providers and cloud subscribers alike.

References


Managing Intrusion Detection as a Service in Cloud Networks

Index Terms

Computer Science
Distributed Computing

Keywords

Cloud Computing; Cre; Intrusion Detection; Saas