Abstract

Cloud Computing is a newly emerged technology. It is getting popularity day by day due to its amazing services. The applications and services based on the cloud are emerging day by day. Due to networked nature of the cloud, resources, data and applications are vulnerable to the attack in cloud environment. So Intrusion Detection Systems (IDS) are employed in the cloud to detect malicious behaviour in the network and in the host. IDS monitors network or host system activities by collecting network information, and analyzes this information for malicious activities and generate alarms, if intrusion takes place. In this paper we surveyed various types of Intrusion Detection Systems proposed over the years for Cloud Computing environment.

References

- Karen Scarfone and Peter Mell 2007, "Guide to Intrusion Detection and Prevention"
A Survey on Intrusion Detection Systems for Cloud Computing Environment

- Hu Zhengbing; Li ZhiTang; Wu Junqi; 2008, "A Novel Network Intrusion Detection System (NIDS) Based on Signatures Search of Data Mining", First International Workshop on Knowledge Discovery and Data Mining, pp. 10-16.
- Tian-rui Li; Wu-ming Pan; 2005, "Intrusion detection system based on new association rule mining model", IEEE International Conference on Granular Computing, pp. 512-515.
A Survey on Intrusion Detection Systems for Cloud Computing Environment


Index Terms

Computer Science Distributed Systems

Keywords

IDS Cloud Computing EDoS attack HIDS NIDS and Signature based IDS; Anomaly based IDS Attacks on Cloud

5 / 6