Abstract

Cloud Computing is defined as a technology that uses internet and there is a central remote server to maintain the data and applications. Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms and are widely used in organizations. Because of their distributed nature, cloud computing environments are easy targets for intruders looking for possible vulnerabilities to exploit. However, with the extensive use of cloud computing, security issues came out on a growing scale. It is necessary to solve these security issues to promote the wider applications of cloud computing. To provide secure and reliable services in cloud computing environment is an important issue. Therefore, a Cloud computing system needs to contain some Intrusion Detection Systems (IDSs) for protecting each virtual machine against threats. In this case there
exists a trade-off between the security level of IDS and the system performance. If the IDS provide stronger security services using more rules or patterns, then it needs much more computational resources in proportion to the strength of security. Another problem in Cloud Computing is that, it is hard to analyse huge amount of logs by system administrators. The objective of the paper is to propose a risk assessment method that enables Cloud Computing System to achieve both effectiveness of using the system resources and strength of the security service without trade-off between them.

References

- Sebastian Roschke, Feng Cheng, Christoph Meinel, "Intrusion Detection in the Cloud&quo;.