Abstract

Cloud computing visualize as the next generation computing technique for Information technology due to advantages provided by this technology. Cloud computing solutions are scalable, advanced and low cost. Its nature is distributed as cloud, it is indefensible to a large category of attacks are very frequent. Security is major challenge in cloud computing. This paper proposed the creation of FVM(forensic virtual machine) so that each virtual machine can be used as different security issue and which security issue have high probability can be classified using Bayesian classifier. An intrusion detection system proposed for monitoring the network against malicious attack. In this paper malicious attacks divided into three major categories first FVM used for detect unauthorized access, second used for malicious nodes and third one for IDS activity.

References

- Monica Nicoli, Stefano Savazzi, Francesca Carminati, Michele Riva, A Bayesian Approach to Device-Free Localisation: Modeling and Experimental Assessment, IEEE Journal Of Selected Topics In Signal Processing, VOL. 8, February 2014.
- Rui Xia, Chengqing Zong, Shoushan Li, Ensemble of feature sets and classification algorithms for sentiment classification, Information sciences 2011.

Index Terms

Computer Science
Distributed Systems

Keywords
Cloud computing  IDS  Bayesian classifier  SVM