Abstract

Cloud Computing is a recent computing model; provides consistent access to wide area distributed resources. It revolutionized the IT world with its services provision infrastructure, less maintenance cost, data and service availability assurance, rapid accessibility and scalability. Grid and Cloud Computing Intrusion Detection System (GCCIDS) detects encrypted node communication and find the hidden attack trial which inspects and detects those attacks that network based and host based can’t identify. It incorporates Knowledge and behavior analysis to identify specific intrusions. Signature based IDS monitor the packets in the network and identifies those threats by matching with database but It fails to detect those attacks that are not included in database. Signature based IDS will perform poor capturing in large volume of anomalies. Another problem is that Cloud Service Provider (CSP) hides the attack that is caused by intruder, due to distributed nature; cloud environment has high possibility for vulnerable resources. By impersonating legitimate users, the intruders can use a service’s abundant resources maliciously. In Proposed System we combine few concepts which are available with new intrusion detection techniques. Here to merge Entropy based System with Anomaly detection System for providing multilevel Distributed Denial of
Service (DDoS). This is done in two steps: First, Users are allowed to pass through router in network site in that it incorporates Detection Algorithm and detects for legitimate user. Second, again it pass through router placed in cloud site in that it incorporates confirmation Algorithm and checks for threshold value, if it's beyond the threshold value it considered as legitimate user, else it's an intruder found in environment. This System is represented and maintained by as third party. When attack happens in environment, it sends notification message for client and advisory report to Cloud Service Provider (CSP).

References

- Sebastian Roschke, Feng Cheng, Christoph Meinel, Intrusion Detection in cloud, Eighth IEEE International Conference on Dependable, Automatic and Secure Computing, PP 729 - 734
- Sumit Kar, An Anomaly Detection Scheme for DDoS Attack in Grid computing, National Institute Of Technology Rourkela, 2009, PP 1 to 49
- Claudio Mazzariello, Roberto Bifulco, Roberto Canonico, Integrating a Network IDS into an Open Source Cloud Computing Environment
- Anukool Lakhina, Mark Crovella, Christophe Diot, Mining Anomalies Using Traffic Feature Distributions, ACM, 2005

Index Terms

Computer Science
Security
Keywords
Cloud computing  Grid Computing  Intrusion detection