Distributed Intrusion Detection System using Mobile Agents in Cloud Computing Environment

Abstract- With the advent of Cloud computing paradigm, the availability of cloud services to users has increased and service costs have reduced by pay-per-use basis. However, security has been a major challenge faced by the cloud due to its open and distributed architecture. Intruders can misuse the cloud resources to achieve their malicious goals. In this paper, we propose a unique security scheme "Distributed Intrusion Detection System using Mobile Agents in Cloud Computing (DIDMACC)" to detect the distributed intrusions in cloud. We have used mobile agents to carry intrusion alerts from consumer virtual machines to the management server where correlation takes place. Our system can detect the intrusions on virtual machines, identify the vulnerable ports, and can correlate malicious events to detect distributed intrusions in a cloud based network. Mobile agents are also used to update the signature database at virtual machines being monitored. Mobile agents, being lightweight and flexible software programs, reduce the network load by carrying intrusion-related data and code. DIDMACC provides a scalable and robust intrusion detection system which is a key requirement for cloud networks. We have validated the security of our system using Ptybull 2.0. The results show that use of mobile agents and correlation has improved the detection of DoS attacks.