

ABSTRACT

Security is the main issue in cloud computing. The main issue security in cloud computing is the attack or threats on the network. There are some examples of attack or security threats, such as port scan, ip spoofing, ping of death, or sniffing packet. Using firewall on the cloud computing is not assured to the security because in the environment of cloud computing where the resource of computation and communication can be accessed together by several users so the attack can come from the infrastructure it self. Effort to detect and analyze every event with suspicion as an attack on the network is by implementing Intrusion Detection System (IDS) on the cloud computing. The positioning of IDS can be placed separated with the cloud server, IDS on the cloud server, and IDS placed on both of them (cloud server and separated with cloud server). In this final project, implementation and analysis was done to know the effect of positioning of IDS to the success of detection and the influence of IDS to the CPU usage and memory on the server cloud. From the analysis there are two alternatives to the positioning of IDS that can detecting every attack on the network. First, IDS was placed on every cloud server with memory usage 4 % and cpu usage 0,1 %. For this alternative can be implemented with assumption if the attack from the outside is less than attack from the inside. Second, IDS was placed separated with cloud server and on the cloud server with memory usage 2 % and cpu usage 0,1 %. For this alternative can be implemented with assumption if the attack from the outside is more than from the inside

Keywords: *cloud computing, security, intrusion detection system*