ABSTRAK

Keamanan merupakan salah satu isu utama dalam *cloud computing*. Isu utama keamanan pada *cloud computing* yaitu serangan atau ancaman pada jaringan. Beberapa contoh serangan atau ancaman terhadap keamanan adalah *port scan*, *ip spoofing*, *ping of death*, maupun paket *sniffing*. Menggunakan *firewall* pada *cloud computing* tidak menjamin keamanannya karena dalam lingkungan *cloud computing* dimana sumber daya komputasi dan komunikasi dapat diakses bersama oleh beberapa pengguna sehingga serangan dapat berasal dari infrastruktur itu sendiri. Upaya untuk mendeteksi dan menganalisis setiap *event* yang dicurigai sebagai serangan pada jaringan yaitu dengan mengimplementasikan *Intrusion Detection System* (IDS) pada *cloud computing*. Peletakkan IDS dapat ditempatkan terpisah dengan server *cloud*, IDS ditempatkan pada server *cloud*, dan IDS ditempatkan pada keduanya (server *cloud* dan terpisah dengan server *cloud*). Pada Tugas Akhir ini, implementasi dan analisis dilakukan untuk mengetahui pengaruh peletakan IDS terhadap keberhasilan deteksi dan juga pengaruh IDS terhadap penggunaan CPU dan memori pada server cloud. Dari hasil analisis terdapat dua alternatif peletakan IDS yang dapat mendeteksi semua serangan pada jaringan yaitu skenario pertama, IDS yang ditempatkan pada setiap server *cloud* dengan beban tambahan penggunaan *memory* 4% dan penggunaan CPU 0,1%. Skenario ini dapat menjadi alternatif jika serangan dari luar lebih sedikit dari serangan dari dalam. Skenario kedua, IDS ditempatkan terpisah dengan server *cloud* dan pada server *cloud* dengan beban tambahan penggunaan *memory* 2% dan penggunaan CPU 0,1%. Skenario ini dapat menjadi alternatif jika serangan dari luar lebih banyak daripada serangan dari dalam.

Kata kunci : *cloud computing*, keamanan, *intrusion detection system*