ABSTRAK

Cloud computing yang ada saat ini banyak membantu karena banyak terhubung satu dengan lainnya menbuat pengguna dimudahkan dalam mengakses layanan yang terdapat di dalam *cloud computing* tanpa harus khawatir oleh jarak dan waktu. Namun ketika sebuah layanan *cloud computing* terhubung satu dengan lainnya muncul masalah terkait keamanan *cloud computing* yang meliputi aspek *confidentiality, integrity* dan *availability* (CIA). Ketika aspek tersebut menjadi topik yang berpengaruh karena ketika sistem *cloud computing* mengalami kebocoran data atau terganggunya kinerja *server* maka akan mengganggu *client* atau *user* ketika memakai layanan *cloud computing*.

Untuk mengatasi permalahan tersebut maka dibangunlah sebuah sistem keamanan yang mengatasi ketiga permasalahan tersebut. Sistem keamanan yang pertama yaitu sebuah *autentifikasi* jaringan menggunakanan Kerberos yang akan dihubungkan dengan server *cloudcomputing*. *Client* yang ingin mengakses layanan cloud computing diharuskan menggunakan aplikasi Kerberos agar bisa masuk kedalam *cloud computing* nya. Sistem selanjutnya yaitu sebuah *Intrusion Prevention System* (IPS). Sebuah sistem yang bekerja dengan cara membaca paket-paket yang dikirimkan ke cloud untuk membaca serangan dari luar.

Pada hasil pengujian baik sistem Kerberos maupun IPS bekerja dengan baik. Setelah melakukan pengujian berupa serangan paket *Flooding* menggunakan ICMP, kemudian IPS memblok hasil paket dan menampilkan hasil *log* dengan baik. Sana dengan Kerberos yang dapat menolak atau memutus koneksi yang bukan dari *client* Kerberos

Kata kunci : Kerberos, IPS, keamanan jaringan, *cloud computing*.