

ABSTRAK

Pesatnya perkembangan teknologi menyebabkan teknologi dapat di pergunakan dalam berbagai bidang. Salah satu penerepan teknologi tersebut adalah dalam sistem keamanan pada jaringan komputer. Penelitian ini membahas implementasi pada pembangunan sebuah keamanan jaringan komputer yang menggunakan komputasi paralel yang digunakan untuk tolak ukur meningkatkan performansi dalam melakukan proses enkripsi dan dekripsi.

Sistem ini bekerja dengan memanfaatkan sebuah kecepatan dari CPU dan GPU dengan metode sistem komputasi paralel yang menunjang performansi dan mempersingkat waktu dalam melakukan sebuah proses enkripsi dan dekripsi data yang dijalankan pada paralel CPU dan GPU dengan menggunakan algoritma AES dan bertujuan mengurangi waktu prosesnya sehingga mendapatkan hasil paralel yang lebih optimal.

Hasil dari penelitian ini menggunakan algoritma AES dengan panjang kunci 256 dapat berjalan melakukan proses enkripsi dan dekripsi menggunakan komputasi paralel pada CPU yang menggunakan *pthread* untuk proses *multicore* dan pada GPU yang menggunakan CUDA. Dalam pengujian menggunakan paralel CPU AES dapat di enkripsi 44,0094 detik dan dekripsi 45,2479 detik yang menggunakan 4 *core* dalam pengujian data 650MB dan jika menggunakan CUDA pada GPU, AES dapat melakukan enkripsi 2,441 detik dan dekripsi 3,898 detik yang menggunakan satu dimensi *block x* sebesar 65535 , *block thread x* sebesar 512.

Kata kunci : AES, Paralel, CPU, GPU, pthread, CUDA