ABSTRACT

The development in technology can be in use in various fields. One application of these technologies are in the security system on a computer network. This research discusses the implementation in the construction of a network security computer that uses parallel computing benchmark which is used to improve performance in the process of encryption and decryption.

The system works by utilizing a speed of the CPU and GPU with system method of parallel computing that support performance and shorten the time to perform a process of encryption and decryption of data that run on parallel CPU and GPU supported by AES algorithm and reduce the processing time and achieve the results more optimal.

Results from this study is the AES algorithm with a key length of 256 can go perform encryption and decryption process using parallel computing on the CPU using pthread for multicore and GPU processes that use CUDA. In testing using a parallel CPU AES can be encrypted and decrypted 45.2479 seconds, 44.0094 seconds seconds using 4 cores in testing and 650MB of data when using CUDA on GPU, AES can perform encryption and decryption 2.441 seconds 3.898 seconds using block dimensions amounted to 65535, thread block x 512.

Keyword : AES, Parallel, CPU, GPU, pthread, CUDA