BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam dunia teknologi komunikasi dan informasi, informasi semakin dimudahkan dengan adanya media telepon hingga internet yang semakin cepat dalam melakukan komunikasi antar manusia maupun informasi penting ataupun tidak. Setelah berkembangnya kemudahan dalam teknologi komunikasi dan informasi hingga kini dirasa penting untuk adanya pengamanan khusus dalam mengamankan informasi dalam komunikasi, karena keamanan suatu sistem merupakan hal yang sangat penting demi menjaga ketersediaan, integritas, dan kerahasiaan data pada suatu institusi atau organisasi. Salah satu cara untuk menjaga tiga aspek dalam keamanan sistem informasi yaitu menggunakan ilmu kriptografi.

Karena semakin banyak yang membutuhkan keamanan sistem maka banyak juga data yang akan dibutuhkan untuk dilindungi dari serangan dari pelaku kriminal oleh karna itu selalu diimbangi dengan teknologi yang semakin mendukung sebuah keamanan data yang sangat besar seperti tenaga komputer dalam kemampuan komputasi yang sangat hebat bahkan dapat berjalan secara paralel sekalipun.

Pada saat ini perkembangan teknologi prosesor sangat kuat seperti yang dimiliki perusahaan raksasa seperti Intel dan Nvidia yang banyak telah dikembangkan atau diukur maupun diuji coba kemampuanya dalam melakukan proses masal dan salah satunya untuk keamanan data. Dua raksasa prosesor ini pun masih mendominasi dalam hal komputasi tercepat pada saat ini.

Dengan berkembang pesatnya teknologi komputasi pada prosesor dari multi prosesor bahkan multi komputer maka semakin banyak proses yang akan dapat bekerja di bawahnya termasuk keamanan data dalam jumlah besar sekalipun. Komputasi paralel adalah salah satu teknik melakukan komputasi secara bersamaan dengan memanfaatkan beberapa komputer secara bersamaan. proses ini umumnya dilakukan saat kapasitas data yang diproses sangat besar, baik karena harus mengolah data dalam jumlah besar ataupun karena tuntutan proses komputasi yang banyak.

1.2 Perumusan Masalah

Rumusan masalah dalam pembuatan Tugas Akhir ini adalah seperti yang dijelaskan di bawah ini:

1. Merancang sistem komputasi paralel dari CPU dan GPU menggunakan algoritma AES-256.
2. Merancang algoritma AES-256 dalam melakukan enkripsi dan dekripsi sebuah data pada sistem komputasi paralel dari CPU dan GPU

1.3 Tujuan

Tujuan dalam pembuatan Tugas Akhir ini adalah seperti yang dijelaskan di bawah ini:

1. Membangun sistem komputasi paralel pada CPU dan GPU menggunakan algoritma AES-256.
2. Mempermudah dan mempercepat proses kerja dari algoritma AES-256 dalam melakukan proses enkripsi dan dekripsi data pada sistem komputasi paralel dari CPU dan GPU.

1.4 Batasan Masalah

Batasan masalah dalam pembuatan Tugas Akhir ini adalah seperti yang dijelaskan di bawah ini:

1. Menggunakan *pthread* untuk melakukan proses paralel pada CPU yang akan menjalankan 4 *core* dalam satu waktu proses enkripsi dan dekripsi pada algoritma AES-256.
2. Menggunakan CUDA untuk melakukan proses paralel dengan satu dimensi *thread* x sebesar 512 dan satu dimensi block x 65535 untuk melakukan proses paralel pada GPU.
3. Membandingan performa dengan mengukur beban proses dan waktu saat melakukan proses enkripsi dan dekripsi data pada CPU dan GPU.

1.5 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Studi Literatur

   Bertujuan untuk mengumpulkan, mempelajari dan memahami materi-materi dasar dan literatur-literatur yang berkaitan dengan GPU,CUDA paralel, CPU, *pthread* paralel, algoritma AES enkripsi dan dekripsi pada algoritma AES-256 dan materi-materi yang digunakan dalam penelitian ini yang bersumber dari berbagai sumber pustaka berupa karya ilmiah, jurnal, *paper*, maupun media elektronik.

2. Analisis dan Perancangan Kebutuhan Sistem

   Merancang sistem yang dibuat, yaitu enkripsi dan dekripsi data yang menggunakan algoritma AES yang akan di implementasikan secara paralel pada GPU yang menggunakan CUDA paralel dan CPU yg menggunakan *pthread*.

3. Implementasi Sistem

   Pada tahap implemetasi ini, program yg dapat melakukan Enkripsi dan dekripsi menggunakan algoritma AES akan di implementasi menggunakan *pthread* paralel untuk menjalankan paralel pada CPU sedangkan perbandingannya menggunakan CUDA paralel untuk menjalankan paralel pada GPU.

4. Pengujian Sistem

   Pada tahap pengujian sistem ini dilakukan pengujian terhadap sistem yang telah dibangun. Hal yang diujikan antara lain yaoiyu pengujian proses *thread* dan *core* yg berjalan saat mengeksekusi enksipsi maupun dekripsi menggunakan system monitor pada ubuntu dan pengujian proses *grid* dan *block* yang berjalan pada saat mengeksekusi enkripsi maupun dekripsi menggunakan *nvidia profiler*.

5. Analisis Hasil Pengujian

   Analisa dari pengujian ini berdasarkan kemampuan sebuah CPU dan GPU yg berjalan secara paralel dalam mengeksekusi sebuah algoritma AES.

6. Penyusunan Laporan Tugas Akhir

   Menyusun laporan penelitian tugas akhir sebagai syarat sidang penelitian.

1.6 Sistematik Penulisan

Penulisan Tugas Akhir ini disusun berdasarkan sistematika sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penelitian.

BAB II DASAR TEORI

Pada bab ini berisi penjelasan tentang Perangkat yang digunakan yaitu Desktop PC yg di dukung nvidia *Graphic* card dan intel CPU, dan menjelaskan tentang CUDA C dan C programming beserta arsitekturnya dan tentang cara kerja *parallel computing* pada GPU dan CPU.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Pada bab ini berisi tentang perancangan sistem, kebutuhan sistem, implementasi AES pada *pthread* pada CPU dan GPU dari segi kebutuhan sistem perangkat keras maupun perangkat lunak pendukung dan proses perancangan jalanya program dalam bentuk diagram.

BAB IV PENGUJIAN DAN ANALISIS

Pada bab ini pengujian dan analisis yang dilakukan pada penelitian ini adalah menguji dan menganalisa proses *core* yg berjalan saat mengeksekusi enksipsi maupun dekripsi menggunakan system monitor pada ubuntu dan pengujian dan analisa proses *grid* dan *block* yang berjalan pada saat mengeksekusi enkripsi maupun dekripsi menggunakan *nvidia profiler*

BAB V KESIMPULAN DAN SARAN

Pada bab ini disampaikan kesimpulan dari penelitian ini dan saran saran untuk penelitian selanjutnya yang merujuk pada penelitian ini.