

ANALISIS DAN IMPLEMENTASI INFRASTRUKTUR HPC CLUSTER MENGUNAKAN MPICH2 PADA SISTEM OPERASI UBUNTU 12.04

Nur Komar¹, R. Rumani², Tengku Ahmad Riza³

¹Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Proses komputasi yang dapat dilakukan oleh komputer telah berkembang dengan pesat. Pada awalnya proses komputasi hanya dapat dilakukan secara sekuensial saja. Sebuah prosesor hanya dapat melakukan sebuah proses saja dan proses yang lain harus menunggu untuk selanjutnya dapat dieksekusi oleh prosesor. Hal tersebut tentu membutuhkan waktu yang lama bagi prosesor untuk mengeksekusi sebuah proses atau melakukan proses komputasi. Akan tetapi seiring perkembangan teknologi mikroprosesor, proses komputasi kini dapat dilakukan secara paralel dengan menggunakan banyak prosesor untuk melakukan sebuah proses komputasi. Penerapan komputasi paralel pada Tugas Akhir ini digunakan untuk cracking password untuk mengetahui kehandalan suatu password.

Teknologi HPC Cluster adalah solusi untuk menjawab mahalnya harga superkomputer. Dengan menggunakan teknologi HPC Cluster kita akan membuat beberapa komputer bekerja sama dalam menjalankan atau menyelesaikan intruksi. Penulis menggunakan MPICH2 sebagai framework untuk membuat komputasi paralel yang nantinya akan membuat beberapa komputer dapat menyelesaikan intruksi cracking password. Serta menggunakan John The ripper untuk cracking password. Penulis menggunakan lima skenario pengujian terhadap fungsional sistem, dekripsi password angka, huruf, kombinasi huruf dan angka, serta cracking user web.

Dari hasil pengujian yang dilakukan, didapatkan hasil untuk pengujian fungsional sistem berjalan dengan baik sesuai dengan yang diharapkan. Pengujian cracking password MD5 angka didapatkan hasil 0.1 menit diuji dengan dekripsi menggunakan satu komputer. Pengujian cracking password MD5 huruf didapatkan hasil 74.54 menit diuji dengan dekripsi menggunakan satu komputer. Pengujian cracking password kombinasi huruf dan angka didapatkan hasil 86.99 menit diuji dengan dekripsi menggunakan satu komputer. Sedangkan untuk cracking user web, didapatkan password user yang di kirim ke server dengan MD5

Kata Kunci : HPC Cluster, MPICH2, Ubuntu 12.04, Cracking password

Telkom
University

Abstract

Computational process that can be done by computer has grown by leaps and bounds. At first the process of computation can only be performed in a sequential manner. A processor can only perform a process only and the others had to wait for the next to be executed by the processor. It certainly took a long time for the processor to execute a process or perform the computation. However, as the development of microprocessor technology, the computing process can now be done in parallel using multiple processors to perform a computational process. Application of parallel computing in this Final used for cracking passwords to determine the reliability of a password.

HPC Cluster technology is the solution to address the high price of supercomputers. Using HPC Cluster technology we will make some computer work together in carrying out or completing instruction. The author uses MPICH2 as parallel computing framework to make that would make some cracking computer passwords can complete instructions. And using John the Ripper for cracking passwords. The authors used five scenarios for functional testing of the system, the decryption password numbers, letters, combinations of letters and numbers, as well as cracking user web.

From the results of the tests performed, the results obtained for the functional testing of the system work as expected. Testing cracking MD5 passwords figure 0.1 minute test results obtained by decryption using one computer. Testing cracking MD5 passwords letter obtained results are tested with 74.54 minutes decrypted using a single computer. Testing cracking password a combination of letters and numbers didapatkan hasil 86.99 minutes was tested by using a decryption komputer. Sedangkan to cracking web user, obtained the user's password is sent to the server with MD5.

Keywords : HPC Cluster, MPICH2, Ubuntu 12.04, Cracking password

BAB I

PENDAHULUAN

1.1 Latarbelakang

Proses komputasi yang dapat dilakukan oleh komputer telah berkembang dengan pesat. Pada awalnya proses komputasi hanya dapat dilakukan secara sekuensial saja. Sebuah prosesor hanya dapat melakukan sebuah proses saja dan proses yang lain harus menunggu untuk selanjutnya dapat dieksekusi oleh prosesor. Hal tersebut tentu membutuhkan waktu yang lama bagi prosesor untuk mengeksekusi sebuah proses atau melakukan proses komputasi. Akan tetapi seiring perkembangan teknologi mikroprosesor, proses komputasi kini dapat dilakukan secara paralel dengan menggunakan banyak prosesor untuk melakukan sebuah proses komputasi. Sebuah komputer dengan ratusan prosesor (*Massively Parallel Processor*) memiliki kemampuan sangat tinggi dalam melakukan proses komputasi.

Akan tetapi sistem dengan ratusan prosesor membutuhkan biaya yang sangat besar. Solusi lain untuk membuat sebuah sistem komputasi yang cepat dan murah adalah dengan membuat sebuah *HPC Cluster* yang digunakan untuk melakukan proses komputasi tertentu secara paralel. Apalagi, sekarang permintaan akan komputasi yang cepat sangat dibutuhkan hampir di semua sektor, baik pendidikan, bisnis, militer, penelitian, maupun kedokteran.

Pada Tugas Akhir ini penulis akan menggabungkan sumber daya dari beberapa komputer, untuk melakukan *Cracking Password*. Kemudian dianalisa sampai sejauh mana peningkatan kecepatan yang terjadi dan sejauh mana sebuah *password* dikatakan aman dari jenis-jenis kombinasi password.

1.2 Rumusan Masalah

1. Apa saja yang dibutuhkan untuk membangun *HPC Cluster*?
2. Bagaimana cara membangun *HPC Cluster* dengan MPICH2?
3. Sejauh mana perbedaan kecepatan *Cracking password* menggunakan satu komputer, dua komputer, tiga komputer, empat komputer?
4. Manakah yang lebih handal antara *password* huruf, angka, atau kombinasi huruf dan angka?

1.3 Batasan Masalah

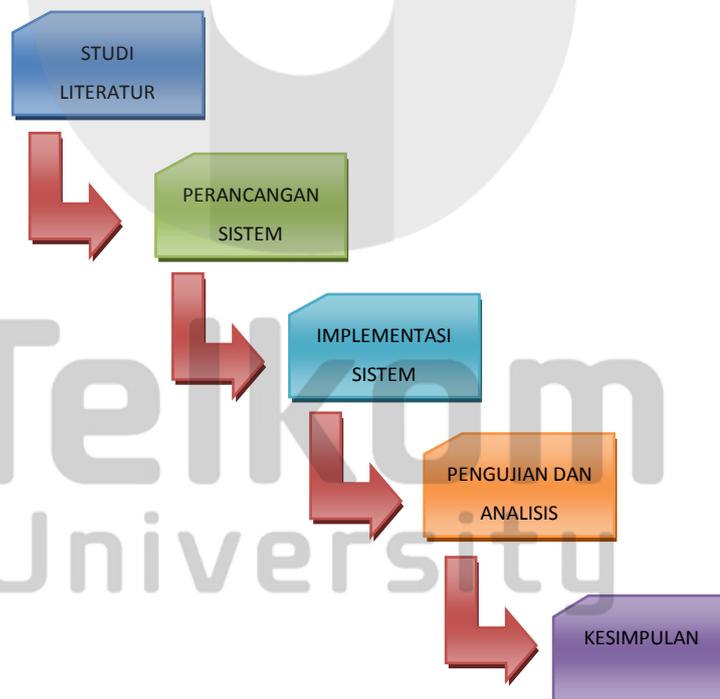
- Lingkungan *Cluster* dibangun pada jaringan LAN(Lokal Area Network)
- Jumlah komputer yang digunakan hanya empat buah
- Tidak berfokus pada sistem keamanan HPC *Cluster*.
- Password yang didekripsi adalah MD5.

1.4 Tujuan

- Mengetahui alat atau *software* yang digunakan untuk membangun HPC *Cluster*.
- Mengetahui cara mengkonfigurasi HPC *Cluster*.
- Meningkatkan pemrosesan komputer yang berguna untuk eksekusi *file* yang membutuhkan pemrosesan yang besar seperti *Cracking password*. Dan Sebagai Awal penelitian Selanjutnya di ittelkom mengenai HPC *Cluster*.
- Mengetahui Keandalan suatu *password* dari kombinasi yang digunakan.

1.5 Metode Penelitian

Untuk mengimplementasikan sistem HPC *Cluster* menggunakan MPICH2, diperlukan tahapan-tahapan yang digunakan dalam menyelesaikan masalah. Untuk tugas akhir ini antara lain:



Gambar 1.1 Metodologi Tugas Akhir

a. Studi Literatur

Di tahap ini dipelajari segala hal mengenai HPC *Cluster* dan MPICH2 dari berbagai sumber hingga dirasa paham untuk membangun HPC *Cluster* menggunakan MPICH2 pada Ubuntu 12.04. Tahapan ini terus dilakukan hingga selesainya Tugas Akhir agar kajian akan Tugas Akhir ini semakin dalam dan dapat mengumpulkan pemahaman-pemahaman dari berbagai sumber hingga ditemukan pemahaman yang tepat bagi penulis.

b. Perancangan Sistem

Di tahap ini digunakan untuk merancang struktur yang akan dibangun agar komputasi paralel dapat berjalan dengan baik. Serta persiapan *software* dan *hardware* yang dibutuhkan juga dibahas di tahap ini.

c. Implementasi Sistem

Di tahap ini dilakukan instalasi , *setting*, dan konfigurasi disisi *node-node* komputasi sehingga terbentuk *Cluster* yang dapat menjalankan MPICH2.

d. Pengujian dan Analisis

Di tahap ini akan diuji apakah sistem dapat berjalan dengan baik dan dapat menjalankan MPI serta dapat melakukan *Cracking Password* dengan *John The Ripper*. Kemudian Jika semua sudah berjalan dengan baik, akan diukur percepatan jika menggunakan beberapa node.

e. Penarikan Kesimpulan

Di tahap ini adalah tahap untuk menyimpulkan Implementasi HPC *Cluster* yang sudah di analisis. Sehingga dapat diketahui parameter atau nilai-nilai yang akan mempengaruhi kinerja HPC *Cluster*.

1.6 Sistematika Penulisan

Adapun sistematika yang digunakan untuk penulisan laporan hasil penelitian Tugas Akhir ini sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas mengenai: latar belakang masalah, perumusan masalah, batasan masalah, tujuan, metodologi penelitian, serta sistematika penulisan dari kegiatan penelitian Tugas Akhir ini.

BAB II DASAR TEORI

Pada bab ini dibahas mengenai teori dasar yang digunakan pada penyusunan Tugas Akhir yang meliputi penjelasan mengenai HPC Cluster, MPICH2, Ubuntu 12.04, NFS, dan SSH.

BAB III PERENCANAAN DAN IMPLEMENTASI SISTEM

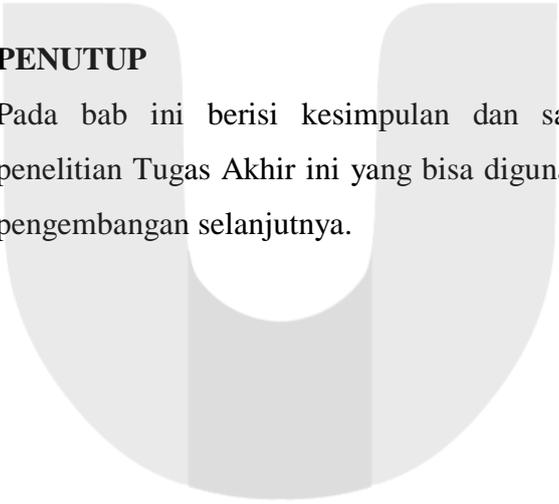
Pada bab ini berisi pembahasan tentang Perencanaan dan Implementasi sistem HPC *Cluster* yang akan dibuat, beserta kebutuhan *hardware* dan *software* yang digunakan.

BAB IV ANALISAN DAN PENGUJIAN SISTEM

Pada bab ini berisi pembahasan tentang analisis dan pengujian terhadap sistem yang telah dibuat.

BAB V PENUTUP

Pada bab ini berisi kesimpulan dan saran dari seluruh kegiatan penelitian Tugas Akhir ini yang bisa digunakan sebagai masukan untuk pengembangan selanjutnya.



Telkom
University

BAB II DASAR TEORI

BAB V

PENUTUP

5.1 KESIMPULAN

Dari perancangan dan pengujian serta analisis yang telah dilakukan maka dapat ditarik kesimpulan bahwa:

1. Penambahan jumlah komputer yang terhubung dalam infrastruktur HPC *Clusters* dapat mempercepat proses *cracking password*. Dapat dilihat hal ini terbukti untuk semua skenario pengujian.
2. Proses *cracking password* angka dapat di dekripsi paling cepat dari jenis-jenis password yang lain seperti huruf dan kombinasi huruf dan angka. Diuji dengan satu komputer didapatkan hasil dekripsi selama 0.1 menit, dua komputer selama 0.05 menit, tiga komputer 0.05 menit, dan empat komputer selama 0.033.
3. Proses *cracking password* huruf lebih handal dari segi keamanan dibandingkan *password* angka dapat dilihat dari hasil uji kehandalan *password* dengan jumlah karakter yang sama memiliki waktu dekripsi untuk satu komputer selama 74.54 menit, dua komputer selama 50.22 menit, tiga komputer 25.81 menit, empat komputer 17.53 menit. Ini dikarenakan kombinasi huruf lebih banyak yaitu sebesar 52 karakter, lebih tinggi dibandingkan angka yang merupakan kombinasi dari sepuluh karakter.
4. Proses *cracking password* kombinasi huruf dan angka dinilai paling handal dari segi keamanan. Terbukti *password* jenis ini memiliki waktu dekripsi paling lama diantara jenis-jenis password lainnya. Satu komputer dapat mendekripsi selama 86.995 menit, dua komputer selama 60.37 menit, tiga komputer selama 33.987 menit, empat komputer selama 23.785 menit. *Password* kombinasi huruf dan angka lebih lama dikarenakan jumlah kombinasi untuk setiap karakter sebanyak 62 karakter.

5.2 SARAN

Berikut saran-saran yang ingin ditunjukkan untuk pengembangan aplikasi dan teknologi HPC *clusters* selanjutnya :

1. Kembangkan HPC *clusters* dengan jumlah komputer yang lebih banyak agar komputasi parallel menjadi semakin besar dan dapat menyelesaikan kasus-kasus yang lebih membutuhkan komputasi kompleks.
2. Buat interface web untuk input *job* seperti kasus grid computing, sehingga memudahkan pengguna awam yang ingin menggunakan aplikasi HPC.
3. Perbanyak penerapan-penerapan aplikasi lain yang memungkinkan dijalankan pada infrastruktur HPC seperti *rendering*, perhitungan matematis yang rumit, dll.



DAFTAR PUSTAKA

1. **Dedy, Syaputra M.** (2011). *Uji kinerja Octave dengan MPITB menggunakan Pustaka Lam/MPI dan OpenMPI*
2. **Dwi, Anton. Mutiara, Benny. Dan Heruseto, Brahmantyo.** (2008). *. Analisis perbandingan antara cluster openmosix dengan mpi terhadap aplikasi rendering pov-ray, universitas. Tugas Akhir: Gunadarma*
3. **Forseth, Lars Daniel.**(2007). *High-Avalability Cluster Support for IBM Informix Dynamic Server (IDS) on Linux.*Thesis: Computer Science, Berufsakademie Stuttgart.
4. **Harindrari, Suryamitra.** (2007). *Pengembangan Portlet.* Fasilkom UI
5. **Komputer, Wahana.**(2009). *Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu 9.* Yogyakarta: Penerbit Andi.
6. **Kurniawan, Agus.**(2010). *Pemrograman Pararel dengan MPI & C.* Yogyakarta:Penerbit Andi.
7. **Makhsun, Ahmad.** (2011). *Implementasi Grid Computing dengan Menggunakan Pengalamatan IPV6.* Proyek Akhir:Jurusan Informatika,Politeknik Elektronika Negeri Surabaya, Institut Teknologi Sepuluh Nopember Surabaya.
8. **Stern, Hal. Eisler, Mike. Dan labiaga Ricardo.**(2008). *Managing NIS and NFS.* , O'Reilly & Associates, Inc
9. **Widyaputra, Guntur.** (2008). *Implementasi Linux Fedora Untuk Pengembangan Cluster.* universitas Gadjah Mada Yogyakarta
10. **Universitas Sumatra Utara.** *Landasan Teori Kriptografi.*ChapterII.
11. <http://www.openwall.com/john/> (diakses 15 januari 2013)