PERANCANGAN ARSITEKTUR SISTEM TERDISTRIBUSI UNTUK PEMECAHAN PASSWORD DENGAN MENGGUNAKAN METODE HYBRID

Skripsi

©UKDW

oleh
ARYONO PRABOWO HADI
22084483

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

PERANCANGAN ARSITEKTUR SISTEM TERDISTRIBUSI UNTUK PEMECAHAN PASSWORD DENGAN MENGGUNAKAN METODE HYBRID

Skripsi

©UKDW

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

ARYONO PRABOWO HADI
22084483

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PERANCANGAN ARSITEKTUR SISTEM TERDISTRIBUSI UNTUK PEMECAHAN PASSWORD DENGAN MENGGUNAKAN METODE HYBRID

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 4 April 2013

ARYONO PRABOWO HADI
22084483

©UKDW

HALAMAN PERSETUJUAN

Judul Skripsi	:	PERANCANGAN ARSITEKTUR SISTEM TERDISTRIBUSI UNTUK PEMECAHAN PASSWORD DENGAN MENGGUNAKAN METODE HYBRID
Nama Mahasiswa	:	ARYONO PRABOWO HADI
N I M	:	22084483
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2012/2013

©UKDW

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 4 April 2013

Dosen Pembimbing I	Dosen Pembimbing II
9/4 2013	
Antonius Rachmat C., SKom.,M.Cs	Willy Sudiarto Raharjo, SKom.,M.Cs

HALAMAN PENGESAHAN

PERANCANGAN ARSITEKTUR SISTEM TERDISTRIBUSI UNTUK PEMECAHAN PASSWORD DENGAN MENGGUNAKAN METODE HYBRID

Oleh: ARYONO PRABOWO HADI / 22084483

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal ....

Yogyakarta, 4 April 2013
Mengesahkan,

Dewan Penguji:
1. Antonius Rachmat C., SKom.,M.Cs
2. Willy Sudiarto Raharjo, SKom.,M.Cs
3. Drs R. Gunawan Santoso, M.Si.
4. Aditya Wikan Mahastama, S.Kom

Dekan,

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi,

(Nugroho Agus Haryono, M.Si)

©UKDW

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas berkat, rahmat, dan karunianya sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "Perancangan Arsitektur Sistem Terdistribusi Untuk Pemecahan *Password* Dengan Menggunakan Metode *Hybrid*" dengan baik.

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu, penulisan laporan Tugas Akhir ini juga bertujuan untuk melatih mahasiswa agar dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan penelitian dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, dan masukkan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Bapak Antonius Rachmat, S.Kom., M.Cs. .selaku dosen pembimbing I yang pertama yang selalu sabar dalam membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
2. Bapak Willy Sudiarto Raharjo, SKom.,M.Cs. selaku dosen pembimbing II yang selalu sabar dan baik membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
3. Keluarga dan saudara yang selalu memberikan doa dan dukungannya kepada penulis dalam menyelesaikan Tugas Akhir.
4. Rekan-rekan penulis yang dengan senang hati memberikan arahan, saran, dan, sharing dalam pengerjaan Tugas Akhir maupun penulisan laporan Tugas Akhir.
5. Pihak lain yang tidak dapat penulis sebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

©UKDW

Penulis menyadari bahwa penelitian dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian.

Akhir kata penulis meminta maaf bila ada kesalahan dalam penyusunan laporan maupun sewaktu penulis melakukan penelitian Tugas Akhir. Semoga penelitian dan laporan Tugas Akhir ini dapat berguna bagi kita semua.

Yogyakarta, April 2013

Penulis

©UKDW

INTISARI

Kemanan data dan informasi mulai berkembang dengan pesat. Salah satu cara untuk pengamanan informasi yaitu dengan menggunakan *password*. *Password* digunakan untuk mencegah orang yang tidak mempunyai otorisasi untuk mengakses informasi tersebut. Sistem keamanan yang berkembang mengharuskan *user* untuk membuat *password* dengan menggunakan kombinasi huruf dan angka. Kombinasi tersebut membuat proses pemecahan *password* membutuhkan *resource*s yang lebih banyak dan komputer yang canggih.

Pada penelitian ini dilakukan perancangan arsitektur sistem terdistribusi untuk memenuhi *resource* yang dibutuhkan oleh proses pemecahan *password*. Sistem ini akan membagi-bagikan beban kerja kepada setiap client, dan client akan melakukan proses pemecahan *password* dengan metode *Hybrid***.** Kehandalan server dibuat dengan metode *Log-based Rollback Recovery* sehingga server bisa mengatasi kegagalan sistem.

Dari hasil penelitian didapatkan bahwa sistem ini dapat memecahkan *password*. Proses pemecahan *password* dapat lebih cepat dengan bertambahnya jumlah client yang terhubung. Berdasarkan pengujian, sistem yang menggunakan 10 *client* dapat memecahkan *password* 73% lebih cepat dibandingkan dengan sistem yang menggunakan 5 *client,*dan sistem yang menggunakan 15 *client* dapat memecahkan *password* 197% lebih cepat dibandingkan dengan sistem yang menggunakan 5 *client.* Sistem *recovery* dengan metode *Log-based Rollback Recovery* dapat mengatasi kegagalan sistem dengan baik. Persentase Tingkat keberhasilan sistem dalam melakukan *recovery* sebesar 100% dengan menggunakan 5 *client*, 10 *client* dan 15 *client*.

Kata Kunci : Sistem terdistribusi, Log-based Rollback Recovery, RMI, Hybrid-Attack.

©UKDW

DAFTAR ISI

©UKDW

©UKDW

©UKDW

DAFTAR GAMBAR

©UKDW

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam perkembangan keamanan di dalam sebuah sistem, banyak program ataupun website yang mengharuskan *user* untuk membuat *password* dengan kombinasi antara huruf, angka, dan juga karakter tertentu. Tujuan dari hal ini adalah sebagai peningkatan keamanan informasi yang ada di dalam sistem. Kenyataannya banyak *user* yang membuat atau mengubah *password* hanya dengan menambahkan angka diantara *password* yang lama. Sebagai contoh, *user* mengganti *password* "user" dengan "user123". Dengan menggunakan pemecah *password* yang ada pada saat ini dibutuhkan waktu dan perangkat yang lebih banyak untuk bisa mendapatkan *password* yang tepat.

Proses pemecahan *password* memerlukan suatu sistem yang dapat memenuhi *resource* yang diperlukan untuk proses pemecahan *password* tersebut, sistem terdistirbusi merupakan solusi yang dapat diterapkan. Sistem terdistribusi adalah kumpulan dari komputer terpisah yang terlihat oleh penggunanya sebagai satu sistem yang saling berhubungan (Tanembaum, 2002). Komputer yang terpisah dapat saling terhubung dengan menggunakan sistem *client* dan server. Sistem di dalam server berfungsi mengatur pendistribusian proses pada setiap komputer, sehingga proses tersebut dapat dilakukan secara bersamaan pada setiap komputer *client*. Dengan menggunakan arsitektur yang diimplementasikan pada sistem terdistribusi ini maka *resource* dari proses pemecahan *password* dapat terpenuhi dan proses pemecahan *password* dapat berjalan dengan lebih cepat.

Pada penelitian akan dibuat arsitektur dan program pemecahan *password* dengan menggunakan sistem terdistribusi mencakup juga proses pendistribusian tugas dari setiap *client*. Sistem terdistribusi dan perancangan arsitektur dari program diharapakan dapat mempercepat proses *hybrid attack* sebagai metode pemecahan *password* sehingga proses dapat berjalan dengan lebih cepat.

©UKDW

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka rumusan masalah dalam penelitian tugas akhir yaitu : Bagaimana menerapkan sistem terdistribusi dan

1. karakter.
2. Proses enkripsi menggunakan algoritma MD5 tanpa penambahan salt.
3. Proses pemecahan *password* menggunakan metode *hybrid attack*.
4. Penambahan berupa karakter pada akhir kata.

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah dapat menerapkan sistem terdistribusi dan membuat arsitektur yang tepat pada program pemecahan *password* agar dapat mendukung proses *hybrid attack* dalam memecahkan *password*. Jika dilihat dari sisi pengguna, penelitian ini dapat membantu *user* dalam melakukan proses pencarian *password* yang hilang dari sebuah sistem dengan lebih cepat.

1.4 Metode Penelitian

Metodologi yang digunakan dalam penelitian ini terdiri dari tahapan sebagai berikut :

1. Studi Pustaka dengan mengumpulkan informasi yang berhubungan dengan arsitekur program, sistem terdistribusi, dan metode *hybrid attack.*
2. Membuat program terdistribusi pemecahan *password* dengan menggunakan metode *hybrid attack*.
3. Melakukan *testing* program dengan :
    a. Memasukkan inputan dengan jumlah karakter minimal dan maksimal untuk melihat perbedaan waktu pemrosesan.
    b. Memasukkan inputan dengan variasi teks yang berbeda untuk melihat perbedaan waktu pemrosesan.

©UKDW

4. Mencatat keluaran dari program berupa waktu yang dibutuhkan untuk memecahkan *password*.
5. Membandingkan hasil keluaran dari program pada setiap proses dengan inputan yang berbeda.
6. Menganalisis dan evaluasi kinerja dari program.

1.5 Sistematika Penulisan

Bab 1 merupakan PENDAHULUAN. Pada bab ini berisi latar belakang masalah yang akan diteliti dan rancangan penelitian yang akan dilakukan. Penelitian ini mengenai pembuatan arsitektur dan program pemecahan *password* secara terdistribusi dengan menggunakan metode *hybrid*.

Bab 2 merupakan TINJAUAN PUSTAKA. Berisi penjelasan teori sistem terdistribusi dan design pattern yang didapat dari berbagai sumber pustaka dan penjelasan tentang konsep dan prinsip-prinsip yang diperlukan untuk membuat program pemecahan *password* dengan menggunakan arsitektur sistem terdistribusi.

Bab 3 merupakan ANALISIS DAN PERANCANGAN SISTEM. Berisi uraian penjelasan mengenai rancangan pembuatan arsitektur dan program pemecahan *password* secara terdistribusi dengan menggunakan metode *hybrid* dan prosedur-prosedur yang ada didalamnya.

Bab 4 merupakan IMPLEMENTASI DAN ANALISIS SISTEM. Berisi pembahasan hasil penerapan pembuatan arsitektur dan program pemecahan *password* secara terdistribusi dengan menggunakan metode *hybrid* pada Bab 3.

Bab 5 merupakan KESIMPULAN DAN SARAN. Berisi kesimpulan-kesimpulan yang didapat setelah melakukan penelitian terhadap pembuatan arsitektur dan program pemecahan *password* secara terdistribusi dengan menggunakan metode *hybrid*. Di samping itu, bab ini berisi saran-saran mengenai pengembangan penelitian ini agar dapat menjadi bahan pertimbangan bagi pembaca yang ingin mengembangkannya di masa mendatang.

©UKDW

BAB 5
KESIMPULAN DAN SARAN

1.1 Kesimpulan

Setelah dilakukan penelitian dan pengujian sistem yang telah dibuat, dapat disimpulkan bahwa :

1. Sistem terdistribusi dengan arsitektur sistem yang telah dibuat dapat diimplementasikan pada proses pemecahan *password*. Sistem terdistribusi dapat membantu mempercepat proses pemecahan *password* dengan membagi-bagi proses pada setiap *client*.
2. Proses checkpoint dan *recovery* dengan menggunakan Log-based *Rollback Recovery* dapat berjalan dengan baik. Proses checkpoint dapat menyimpan *state* pada file log dan mengembalikan sistem seperti pada *state* sebelumnya melalui proses *recovery*. Persentase tingkat keberhasilan recovery sistem sebesar 100% pada sistem dengan menggunakan 5 *client*, 10 *client* dan 15 *client*.
3. Sistem yang menggunakan 10 *client* dapat memecahkan *password* 73% lebih cepat dibandingkan dengan sistem yang menggunakan 5 *client,*dan sistem yang menggunakan 15 *client* dapat memecahkan *password* 197% lebih cepat dibandingkan dengan sistem yang menggunakan 5 *client.*

1.2 Saran

Untuk pengembangan lebih lanjut, saran yang dapat diberikan adalah sebagai berikut :

1. Untuk penelitian selanjutnya dapat diimplemetasikan sistem pemecahan *password* dengan menggunakan prosesor pada GPU untuk mempercepat pemecahan *password*.
2. Perlu dilakukan implementasi mutithreading di sisi client untuk mempercepat proses pemecahan pemecahan *password*.
3. Perlu dilakukan studi lebih lanjut tentang penggunaan wordlist, dan pembuatan wordlist yang efektif didalam proses pemecahan *password*.

©UKDW

DAFTAR PUSTAKA

Crumpacker, J.R (2009). Distributed *Password* Cracking. California : Naval Postgraduate School.

Dokumentasi RMI. http://docs.oracle.com/javase/6/docs/technotes/guides/rmi/index.html di akses tanggal 10 Januari 2013.

Elnozahy, M , Alvisi, L , Wang, Y , Johnson, D.B (1999). A Survey of Rollback-Recovery Protocols in Message-Passing System. Pittsburgh : Carnegie Mellon University.

Ksemkalyani,A.D & Singhal, M (2008). Distributed Computing : Principles, Algorithms, and Systems. Cambridge : University Press.

Library Joda-Time. http://joda-time.sourceforge.net/ diakses tanggal 10 januari 2012.

Lim, Ryan (2004). Parallelization of John the Ripper (JtR) Using MPI. Lincoln, University of Nebraska.

Reilly, D & Reilly, M (2002) Java™ Network Programming and Distributed Computing, Boston : Pearson Education, Inc.

Tanembaum, A.S & Steen, V.M (2002). Distributed System : Principles and Paradigms. Prentice Hall.

Tutorial RMI. http://docs.oracle.com/javase/tutorial/rmi/ di akses tanggal 10 Januari 2013.

Zonenberg, A (2010). Distributed Hash Cracker: A Cross-Platform GPU-Accelerated *Password* Recovery System. New York : Rensselaer Polytechnic Institute.

©UKDW