

BAB I

PENDAHULUAN

1.1 Latar Belakang

Adopsi teknologi komunikasi dan informasi telah mengubah paradigma pengelolaan data dari analog menjadi digital. Perubahan ini membawa berbagai keuntungan, seperti pengolahan data yang semakin mudah, media penyimpanan data yang lebih ringkas, pengiriman data semakin cepat, dll. Namun dibalik semua keuntungan ini terselip bahaya yang mengincar data. Pihak yang tidak berhak dapat dengan mudah mengakses data yang bersifat rahasia.

Berbagai upaya telah dilakukan untuk mengamankan data, terutama yang sifatnya rahasia. Penggunaan firewall di jaringan untuk mencegah penyusup masuk ke dalam jaringan internal, kebijakan yang mengharuskan pengguna memilih password yang tidak mudah ditebak, hingga penggunaan antivirus untuk mencegah penyalahgunaan data oleh perangkat lunak berbahaya. Namun sering kali semua upaya ini belum cukup, ketika misalnya penyusup mendapatkan akses secara fisik ke sistem maka ia dapat dengan mudah mengakses data-data rahasia.

Salah satu metode yang dapat digunakan untuk mengamankan data adalah kriptografi. Kriptografi dapat mengubah data menjadi suatu bentuk yang tidak dapat dimengerti oleh pihak yang tidak berhak, bahkan ketika pihak tersebut mendapatkan akses fisik ke sistem.

Beberapa penelitian telah dilakukan menggunakan algoritma kriptografi DES[2, 3, 4, 5], AES[6, 7], dan Blowfish[6, 8] untuk melakukan enkripsi terhadap data yang disimpan di *filesystem*. DES tidak lagi disarankan untuk digunakan dalam aplikasi kriptografi karena terbukti tidak aman dari berbagai serangan kriptanalisis. AES hingga saat ini dianggap sebagai salah satu algoritma yang paling aman namun sangat lambat dalam proses komputasi. Di lain pihak, Blowfish merupakan algoritma enkripsi kunci simetris yang sangat cepat dan aman[9]. Blowfish sangat cocok diterapkan pada sistem kriptografi di mana kunci yang digunakan tidak terlalu sering berubah, seperti pada pengenkripsi file secara otomatis pada *filesystem*.

Dalam Tugas Akhir ini dilakukan penelitian untuk mendisain dan mengimplementasikan suatu filesystem terenkripsi yang dibangun di

atas *framework* FUSE. *Filesystem* ini melakukan enkripsi dan dekripsi pada semua data yang disimpan di dalamnya. Akses terhadap data tersebut hanya dapat dilakukan jika pengguna dapat memasukkan kunci yang sesuai.

Penggunaan kriptografi di level *filesystem* ini dapat meningkatkan keamanan data, sehingga data-data rahasia yang dimiliki pengguna tidak jatuh ke tangan pihak lain.

1.2 Rumusan Masalah

Masalah yang diteliti dalam Tugas Akhir ini adalah:

- a) Bagaimana memanfaatkan *framework* FUSE untuk membangun *filesystem* yang dapat berjalan di atas sistem operasi Linux yang dapat melakukan enkripsi dan dekripsi menggunakan algoritma Blowfish.
- b) Bagaimana membangun aplikasi berbasis GUI yang dapat melakukan operasi *filesystem* terenkripsi.

1.3 Tujuan dan Manfaat

Tujuan dari penelitian Tugas Akhir ini adalah:

- a) Mendisain dan mengimplementasikan *filesystem* berbasis FUSE yang dapat melakukan enkripsi dan dekripsi terhadap file pada sistem operasi GNU/Linux.
- b) .Membangun aplikasi berbasis GUI untuk melakukan operasi pada *filesystem* terenkripsi.

Manfaat dari penelitian Tugas Akhir ini adalah memberikan solusi pengamanan data berupa perangkat lunak yang dapat digunakan untuk melakukan enkripsi dan dekripsi terhadap data secara otomatis dan transparan.

1.4 Batasan Masalah

Filesystem dalam penelitian Tugas Akhir ini dikembangkan di lingkungan sistem operasi GNU/Linux dengan kernel versi 2.6. *Filesystem* dibangun di level *user space* dengan menggunakan *framework* FUSE. Enkripsi dan dekripsi data yang disimpan di media penyimpanan dilakukan dengan menggunakan algoritma Blowfish menggunakan pustaka libgcrypt. *Filesystem* ini dapat berjalan dengan

baik pada sistem operasi Ubuntu 10.04 64 bit.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian Tugas Akhir ini adalah:

- a) Studi Literatur
Pada tahap ini akan dilakukan pencarian jurnal, paper, prosiding, buku, dan dokumentasi yang berkaitan dengan permasalahan penelitian dalam Tugas Akhir.
- b) Disain Sistem
Pada tahap ini akan ditentukan disain sistem seperti apa yang akan digunakan sesuai dengan tujuan penelitian.
- c) Implementasi
Tahapan ini bertujuan untuk menuliskan kode pemrograman dari sistem yang dibuat.
- d) Uji Coba
Melakukan uji coba terhadap sistem yang sudah jadi, dengan melakukan simulasi serangan berupa pembuatan file yang akan dienkripsi oleh sistem. Tahapan ini juga mencakup uji coba kemampuan perbandingan kecepatan penulisan file ke harddisk dengan beberapa file system yang ditentukan kemudian di bab selanjutnya.
- e) Penyusunan Laporan
Pada tahapan ini dilakukan dokumentasi terhadap seluruh kegiatan penelitian untuk dijadikan sebagai laporan penelitian Tugas Akhir.

1.6 Sitematika Penulisan Laporan

Penulisan laporan hasil penelitian Tugas Akhir ini dibagi menjadi lima bagian yang dapat diuraikan sebagai berikut:

- | | |
|--------|---|
| BAB I | Pendahuluan yang menguraikan tentang latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, metodologi penelitian, dan sistematika penulisan laporan. |
| BAB II | Penjelasan tentang berbagai teori penunjang yang digunakan dalam melakukan penelitian. Cakupan pembahasan dalam bab ini meliputi konsep kriptografi, |

sistem operasi GNU/Linux, konsep algoritma Blowfish, *framework File System On Userspace* (FUSE), dan penelitian terkait.

BAB III Analisis dan perancangan sistem yang akan diteliti. Bahasan di bab ini meliputi kebutuhan perangkat keras dan perangkat lunak pendukung, serta rancangan sistem yang dibuat,.

BAB IV Bagian ini membahas tentang implementasi dari sistem yang telah dirancang pada bagian sebelumnya. Pembahasan di bab ini meliputi penulisan kode program untuk masing-masing komponen. Di bab ini juga akan dilakukan analisis dan uji coba kinerja dari sistem yang diteliti.

BAB V Di bab ini diuraikan kegiatan-kegiatan yang telah dilakukan dalam bentuk kesimpulan dan saran-saran untuk perbaikan terhadap sistem yang telah dibuat.