BAB 1

Pendahuluan

1.1 Latar Belakang Masalah

PT. Prospera Consulting Engineers merupakan salah satu perusahaan konsultan yang telah cukup dikenal di Indonesia yang berdiri pada tahun 1980 yang bergerak dalam bidang jasa konsultasi teknik. Seiring dengan bertambahnya permintaan/kebutuhan akan jasa konsultasi, layanan yang diberikan kemudian berkembang menjadi lebih luas lagi, mulai dari perencanaan umum, jasa survei, studi kelayakan, perencanaan teknis, umum, transportasi, pariwisata, pos dan telekomunikasi, pertanian, perindustrian, pertambangan dan energi, serta bidang-bidang lain.

Saat ini PT. Prospera Consulting Engineers menghadapi masalah dalam keamanan data atau informasi yang bebas diakses oleh berbagai pihak dalam perusahaan. Data atau dokumen yang perlu dijaga kerahasiaannya, antara lain data atau dokumen keuangan perusahaan, data strategi pengembangan usaha perusahaan, dan data atau informasi hasil survei/studi kelayakan, serta data atau informasi perencanaan umum/teknis. Rusak atau hilangnya data hasil penelitian yang diperoleh dengan waktu yang cukup lama dan biaya yang tinggi oleh virus juga tentu saja sangat tidak diinginkan terlebih lebih bila data tersebut merupakan data atau informasi pengembangan usaha atau industri yang strategis.

Untuk menghindari terjadinya kejahatan dan kerugian dalam komputer, maka diperlukan suatu keamanan yang baik sehingga data yang terdapat pada

komputer menjadi lebih aman. Salah satu caranya adalah dengan kriptografi menggunakan algoritma *Rijndael* dan kompresi menggunakan algoritma LZW.

Algoritma *Rijndael* bisa diterapkan pada lingkungan perangkat keras yang terbatas. Terbukti pada *smart card* hanya butuh memori sebesar 66 *bytes* untuk proses enkripsi ataupun dekripsinya, masih lebih baik dari algoritma RC6 yang membutuhkan memori sebesar 156 *bytes* untuk proses enkripsi dan dekripsinya. Algoritma Rijndael beroperasi dalam *byte*, bukan dalam *bit*. Dengan kunci sepanjang 128 *bit*, 192 *bit*, dan 256 *bit*, maka jumlah perputarannya antara 10 ronde, 12 ronde, dan 14 ronde. [14]

Algoritma *Lempel-Ziv-Welch* (LZW) memiliki rasio kompresi 60,2% dibandingkan dengan algoritma *Huffman* yang memiliki rasio kompresi 71,4%. Algoritma ini melakukan kompresi dengan menggunakan kamus, dimana fragmen-fragmen teks digantikan dengan indeks yang diperoleh dari sebuah kamus. Pendekatan ini bersifat adaptif dan efektif karena banyak karakter dapat dikodekan dengan mengacu pada string yang telah muncul sebelumnya dalam teks. Prinsip kompresi tercapai jika referensi dalam bentuk pointer dapat disimpan dalam jumlah bit yang lebih sedikit dibandingkan string aslinya. [15]

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah tersebut dapat dibuat suatu rumusan masalah, yaitu:

Bagaimana cara mengimplementasikan algoritma kriptografi *Rijndael* dan algoritma kompresi LZW untuk berkas digital di PT. Prospera Consulting Engineers?

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah membangun perangkat lunak enkripsi dan kompresi data untuk PT. Prospera Consulting Engineers berbasis *desktop*.

Sedangkan tujuan dari penelitian ini adalah:

1. Memberikan keamanan data untuk para pengguna.
2. Mencegah akses dari pihak yang tidak berhak mengetahui data-data penting perusahaan.
3. Mencegah data rusak akibat terinfeksi virus.
4. Memampatkan data terenkripsi atau tidak terenkripsi.

1.4 Batasan Masalah

Agar fokus penelitian ini terjaga, diberikan beberapa batasan sebagai berikut:

1. Metode enkripsi yang digunakan adalah kunci-simetris dengan algoritma kriptografi *Rijndael*.
2. Metode kompresi yang digunakan, yaitu metode *dictionary* dengan algoritma kompresi *lossless Lempel-Ziv-Welch* (LZW).
3. Aplikasi ini berbasis *desktop* dan dapat digunakan pada semua tipe berkas atau *file*, seperti dokumen, musik, gambar, atau video.
4. Aplikasi ini hanya digunakan untuk satu pengguna pada setiap komputer.
5. Ukuran *file* yang digunakan untuk pengujian berkisar antara 15 MB-40 MB.

1.5 Metodologi Penelitian

Metodologi yang digunakan pada penelitian adalah metodologi kualitatif deskriptif analitis, yaitu metodologi penelitian yang melakukan penuturan, analisis

dan mengklasifikasikan data dan informasi yang diperoleh dengan berbagai teknik seperti survey, wawancara, observasi, angket, kuesioner, studi kasus, dan lain-lain [5]. Dalam hal ini penelitian deskriptif kualitatif akan lebih difokuskan kepada peneltian kondisi sekarang yang dibagi menjadi dua tahap, yaitu:

1. Tahap Pengumpulan Data

   Tahap pengumpulan data yang dilakukan dalam penelitian dibagi menjadi dua teknik, yaitu:

   a. Studi Pustaka

      Studi pustaka adalah mempelajari referensi-referensi dan data yang berhubungan dengan permasalahan yang akan dibahas dengan bersumber pada buku-buku, serta bacaan lain yang kiranya dapat membantu untuk menyelesaikan pembangunan sistem informasi ini ini.

   b. Studi Lapangan

      Studi lapangan adalah tahap pengumpulan data secara langsung, baik secara observasi maupun wawancara. Adapun penjelasan mengenai observasi dan wawancara sebagai berikut:

      1. Observasi

         Observasi adalah pengamatan langsung kepada para pembuat keputusan berikut lingkungan fisiknya dan atau pengamatan langsung suatu kegiatan yang sedang berjalan. Observasi yang dilakukan yaitu dengan mengamati secara langsung bagaimana proses baca dan olah data serta pengamanan data yang berlangsung sekarang ini di PT. Prospera Consulting Engineers.

2. Wawancara (*Interview*)

   Wawancara adalah suatu percakapan langsung dengan tujuan-tujuan tertentu dengan menggunakan format tanya-jawab yang terencana. Wawancara dilakukan yaitu kepada Bapak Mochamad Wibowo Tri Lumaksono, S.Kom yang menjabat sebagai koordinator IT di PT. Prospera Consulting Engineers dan pihak-pihak terkait lainnya yang berhubungan dengan pembangunan sistem.

2. Tahap Pembangunan Perangkat Lunak

   Tahap pembangunan perangkat lunak yang dilakukan menggunakan model *Waterfall* seperti pada Gambar 1.1 yang mempunyai lima tahapan, yaitu [6]:

   1. *Requirements Analysis and Definition*

      Mengumpulkan kebutuhan secara lengkap kemudian kemudian dianalisis dan didefinisikan kebutuhan yang harus dipenuhi oleh program yang akan dibangun. Fase ini harus dikerjakan secara lengkap untuk bisa menghasilkan desain yang lengkap.

   2. *System and Software Design*

      Desain dikerjakan setelah kebutuhan selesai dikumpulkan secara lengkap.

   3. *Implementation and Unit Testing*

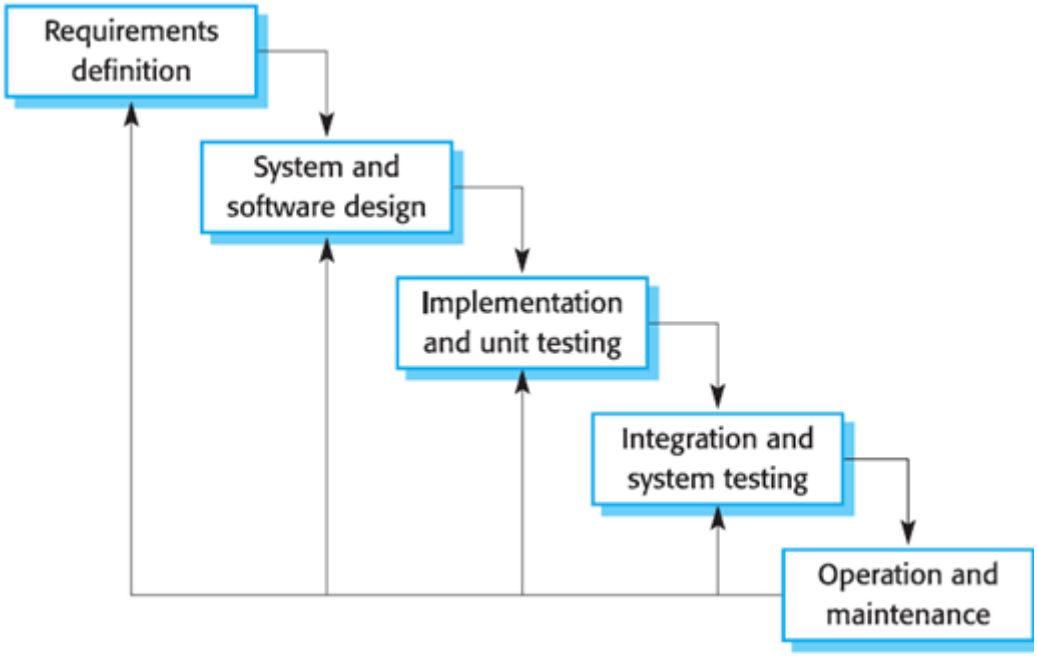
      Desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemrograman yang sudah ditentukan. Program yang dibangun langsung diuji baik secara unit.

   4. *Integration and System Testing*

      Penyatuan unit-unit program kemudian diuji secara keseluruhan.

5. *Operation and Maintenance*

   Mengoperasikan program di lingkungannya dan melakukan pemeliharaan, seperti penyesuaian atau perubahan karena adaptasi dengan situasi sebenarnya.



Gambar 1.1 Model *Waterfall* [6]

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

Bab 1 Pendahuluan

Menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan pembatasan masalah, metodologi penelitian, serta sistematika penulisan.

Bab 2 Tinjauan Pustaka

Membahas sejarah instansi terkait serta berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernah dilakukan sebelumnya termasuk sintesisnya.

Bab 3 Analisis dan Perancangan Sistem

Menganalisis masalah dan merancang model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti serta model matematis untuk analisis dan perancangannya.

Bab 4 Implementasi dan Pengujian Sistem

Merupakan tahapan yang dilakukan dalam penelitian secara garis besar sejak dari tahap persiapan sampai penarikan kesimpulan, metode dan kaidah yang diterapkan dalam penelitian. Termasuk menentukan variabel penelitian, identifikasi data yang diperlukan dan cara pengumpulannya, penentuan sampel penelitian dan teknik pengambilannya, serta metode/teknik analisis yang akan dipergunakan dan perangkat lunak yang akan dibangun.

Bab 5 Kesimpulan dan Saran

Berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir.