BAB I

PENDAHULUAN

1. 1. Latar Belakang Masalah

Perusahaan yang saat ini bernama PT. Citra Bumi Madani pada dasarnya mulai melakukan kegiatan pada tahun 1993. Pada awal kegiatannya perusahaan ini belum mempunyai badan hukum, melainkan lebih merupakan suatu kegiatan usaha di bidang survey pemetaan yang bersifat pribadi / partikelir (individual / personal). Selain menyediakan jasa di bidang survey pengukuran, perusahaan ini juga menyediakan jasa trainer untuk melatih personil dibidang survey pemetaan, terutama dalam melatih pengoperasian alat-alat pengukuran type terbaru maupun metoda-metoda pengukuran baru. Seiring dengan hal tersebut, maka asset dalam bentuk peralatan dan juga jumlah personil juga semakin bertambah diperlukan penataan organisasi dan manajemen yang lebih baik. Dari tahun ketahun kepercayaan pengguna jasa dibidang pengukuran terhadap perusahaan ini semakin meningkat, khususnya permintaan jasa pengukuran dari perusahaan-perusahaan yang bergerak dibidang tambang seperti tambang batubara, tambang galena dan tambang nikel yang tersebar di seluruh indonesia.

Sistem yang sedang berjalan saat ini pengiriman dokumen antar bagian masih sangat manual, yaitu dengan cara memberikan dokumen secara langsung kepada

bagian yang dituju. Cukup menghabiskan waktu dalam pengerjaannya dan itegritas dokumen itu pun belum bisa terjaga dengan baik.

Hal tersebut menimbulkan suatu masalah yaitu bagaimana membuat sistem agar dokumen yang akan dikirm asli dari pengirim aslinya dan mengetahui siapa pengirimnya. Maka solusinya adalah membuat sistem untuk mengetahui keaslian dokumen, dengan membuat sistem aplikasi *digital signautre.* Perangkat yang akan dibangun adalah pembuatan *digital signature* untuk pesan yang akan dikirmkan. Jadi, sebelum pesan dikirimkan terlebih dahulu akan dibuatkan *digital signature* (tanda tangan digital) untuk menjaga keaslian pesan tersebut. Pembuatan *digital signature* ini akan dilakukan pada jaringan LAN (*Local Area Network*) PT. Citra Bumi Madani saja, yang artinya hanya di lakukan di wilayah PT. Citra Bumi Madani.

Pengertian *Digital Signature* itu adalah sebuah metode dalam dunia kriptografi yang berguna untuk menjaga keotentikan, integritas, dan nirpenyangkalan suatu dokumen digital, sehingga mencegah adanya pemalsuan atau modifikasi dari pihak luar yang tidak berwenang. Yang dimaksud dengan tanda tangan digital bukanlah tanda tangan yang di-digitisasi dengan alat *scanner,* tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengiriman pesan (hal ini kontras dengan tanda tangan pada dokumen kertas yang bergantung hanya pada pengiriman dan selalu sama untuk semua dokumen). Dengan tanda tangan digital, maka integritas data dapat dijamin, disamping itu ia juga digunakan untuk membuktikan asal pesan (keabsahan pengirim), dan nirpenyangkalan.

Perangkat lunak ini dibuat dengan menggunakan fungsi HASH SHA-256 dan metode *verifiable ring signature*. Fungsi HASH SHA-256 ini memilki kelebihan yaitu tidak ditemukannya *collision* pada fungsi tersebut. Begitu pula dengan metode *verifiable ring signature* mempunyai beberapa kelebihan yaitu pihak penerima mengetahui bahwa pesan tersebut dikirim oleh sekumpulan orang yang tergabung dalam lingkar kerahasiaan tersebut, dan bisa mengetahui siapakah individu yang mengirimkan pesan tersebut.

Berdasarkan uraian di atas, penulis bermaksud untuk mengambil tugas akhir (skripsi) dengan judul " Pembuatan *Digital Signature* Pada Dokumen Menggunakan Metode *Verifiable Ring Signature* di PT. Citra Bumi Madani".

1. 2. Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka yang menjadi permasalahan adalah bagaimana pesan dapat dipastikan asli dari pengirim aslinya dan pesan tersebut aman.

1. 3. Maksud dan Tujuan

1. 3. 1. Maksud

Maksud dari penulisan tugas akhir ini adalah untuk membangun perangkat lunak yang dapat membuat *digital signature* menggunakan metode *verifiable Ring Signature* untuk memastikan pesan tersebut asli.

1. 3. 2. Tujuan

Adapun tujuan dari tugas akhir ini adalah sebagai alat yang mempermudah dalam melakukan pengiriman dokumen antar bagian dalam perusahaan.

1. 4. Batasan Masalah

Ruang lingkup dalam perancangan dan pembuatan perangkat lunak pembuatan *digital signature* meliputi :

1. File dokumen yang dikirimkan tidak boleh lebih dari 25 MB.
2. File yang bisa dibaca oleh aplikasi adalah file dengan format (.txt) dan (.doc)
3. Dokumen yang akan dikirim adalah surat pesetujuan peminjaman alat, dan laporan bukti pernyataan
4. Penyampaian informasi Pembuatan *digital signature ini* hanya pada jaringan LAN (*Local Area Network*) di PT. Citra Bumi Madani.
5. Metode pembuatan *digital signature ini* menggunakan *Verifiable Ring Signature.*
6. Penggunaan hashing menggunakan SHA-256.
7. Aplikasi dibuat menggunakan *Java2 Standard Edition* (*J2SE).*
8. Metode perangkat lunak digunakan pemodelan *Objeck Orientied Programming* (OOP).
9. Pemodelan objek menggunakan *tools Rational Rose* 2000.

1. 5. Metodologi Penelitian

Metodologi penelitian yang digunakan untuk membangun perangkat lunak ini menggunakan metode analisis deskriptif yaitu suatu metode yang bertujuan untuk mendapatkan gambaran yang jelas tentang hal-hal yang diperlukan, melalui tahapan sebagai berikut :

1. 5. 1. Pengumpulan Data

Metode pengumpulan data merupakan suatu metode atau cara untuk mendapatkan data-data yang dibutuhkan. Metode yang digunakan adalah :

1. Studi Pustaka

Studi pustaka adalah pencarian referensi–referensi yang berhubungan dengan penyusunan tugas akhir, baik melalui internet ataupun buku–buku referensi yang meliputi *digital signature.* Berdasarkan referensi yang telah terkumpul, dapat diambil kesimpulan mengenai perancangan sistem, teknik pengerjaan, maupun metode–metode apa saja yang akan digunakan dalam penyelesaian tugas akhir ini. Pada tahap ini dilakukan pendalaman buku-buku *literature* yang berhubungan dengan *Verifiable Ring Sigature*. Serta berbagai macam materi tentang konsep pemrograman *Java*.

2. Studi Dokumentasi

Studi dokumentasi adalah mempelajari dokumentasi yang disusun dalam pembuatan suatu aplikasi. Pada umumnya, dokumentasi membahas fungsi dari masing-masing elemen aplikasi untuk mempermudah pengguna dalam pemakaian aplikasi atau membahas tentang langkah-langkah pembuatan suatu aplikasi beserta

catatan-catatan yang disertakan. Studi dokumentasi lebih banyak digunakan dalam implementasi.

1. 5. 2. Pembangunan Perangkat Lunak

Metode penelitian yang digunakan adalah model Sequensial Linear. Secara umum, tahap-tahap penelitian dalam model Sequensial Linear adalah :

1. Analisis Kebutuhan

Analisis kebutuhan meliputi penentuan perangkat lunak, penentuan perangkat keras yang sesuai dengan perangkat lunak dan aplikasi yang hendak dibuat, dan data-data yang diperlukan untuk membuat aplikasi.

2. Desain sistem dan perangkat lunak

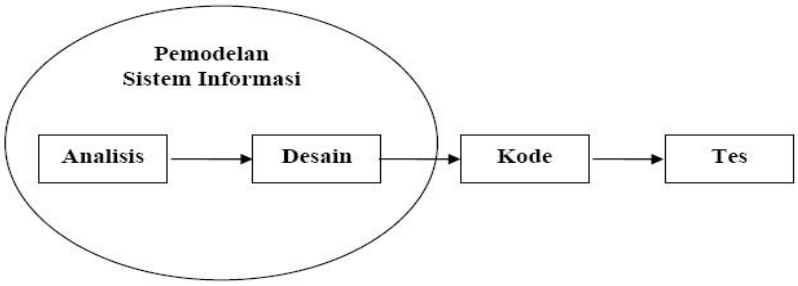
Pada tahap ini, langkah awal yang dilakukan adalah membuat rancangan sistem secara keseluruhan. Setelah itu setiap item akan diperjelas dengan detail-detail proses, beserta target yang akan dicapai pada tiap-tiap prosesnya.

3. Implementasi

Sistematika pembuatan perangkat lunak, disesuaikan dengan desain yang telah ditentukan pada tahap perancangan. Tahapan ini meliputi, *coding*, implementasi algoritma, serta implementasi terhadap hasil-hasil yang diperoleh dari referensi. Pembuatan perangkat lunak ini akan dikerjakan menggunakan bahasa pemrograman Java, serta menggunakan sistem operasi Windows XP, sedangkan untuk implementasinya menggunakan *NetBeans IDE 6.8*.

4. Pengujian

Pada tahap ini penulis melakukan pengujian terhadap sistem yang telah dibuat dan melakukan analisa dengan mempertimbangkan kemungkinan kesalahan yang terjadi baik dari waktu pengenalan, waktu pengiriman, keakuratan pengenalan, dan keakuratan pemetaan.



Gambar 1.1 ***Sequensial Linear Model***

1. 6. Sistematika Penulisan

Bab I. Pendahuluan

Bab ini menjelaskan secara singkat mengenai latar belakang, perumusan masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, sistematika penulisan.

Bab II. Tinjauan Pustaka

Berisi teori-teori pendukung dalam membangun perangkat lunak. Seperti metode *Verifiable Ring Signature*, SHA-256 dan teori mengenai J2SE juga NetBeans IDE 6.8.

Bab III. Analisis dan Perancangan Sistem

Berisi tentang analisis dan perancangan antarmuka untuk perangkat lunak yang akan dibangun. Pemodelan berorientasi objek menggunakan *tools* Rational Rose 2000

Bab IV. Implementasi Dan Pengujian Sistem

Berisi implementasi dari hasil analisis dan perancangan, serta hasil pengujian perangkat lunak.

Bab V. Kesimpulan Dan Saran

Berisi tentang kesimpulan yang dapat diambil dan saran-saran yang dapat diberikan untuk pengembangan perangkat lunak lebih lanjut.