

BAB 1

PENDAHULUAN

1.1 Latar Belakang

PT. BARATIM INFO BUMI merupakan perusahaan yang bergerak di bidang Geoinformation Technology yang memberikan layanan kepada masyarakat luas baik kepada dunia usaha dan masyarakat umum secara efisien, cepat, akurat, dan terkontrolserta terintegrasi dengan inovasi - inovasi terkini. PT. Baratim Info Bumi memiliki masalah yaitu sering hilangnya data penting yang disebabkan oleh kurangnya keamanan terhadap data penting tersebut. Hilangnya data penting dapat terjadi melalui beberapa hal salah satunya yaitu berbagi file sembarangan. Untuk saat ini karyawan PT. Baratim Info Bumi dalam berbagi file masih menggunakan hardisk eksternal. Kurangnya kesadaran keamanan data dapat membuat seseorang dengan sangat mudah membawa ancaman pencurian terhadap data penting yang ada pada perusahaan. Pencurian data yang ada diperusahaan dapat datang dari mana saja baik dari ruang lingkup perusahaan ataupun dari luar ruang lingkup perusahaan. Pernah terjadi kasus ketika seorang karyawan berbagi file menggunakan hardisk eksternal yang menyebabkan kehilangan data penting yang ada diperusahaan. Kehilangan data penting tersebut terjadi kepada beberapa pc yang ada diperusahaan karena permasalahan tersebut menyebar begitu cepat kepada pc karyawan lain. Dengan adanya permasalahan tersebut PT. Baratim Info Bumi menginginkan data penting yang ada pada perusahaan lebih dibungkus menggunakan enkripsi agar menjadi lebih aman. Oleh karena itu dibutuhkan sebuah sistem yang difokuskan mampu menjaga keamanan data penting yang ada diperusahaan dari ancaman orang yang tidak bertanggung jawab.

Keamanan adalah suatu proses yang sangat penting untuk menjaga kerahasiaan data dan informasi dari orang-orang yang tidak bertanggung jawab. Pada zaman yang sudah serba digital seperti saat ini keamanan memiliki beberapa jenis keamanan seperti keamanan data, keamanan jaringan, keamanan komputer dan berbagai macam keamanan lainnya. Keamanan semakin berkembang karena pada saat ini tidak sedikit perusahaan yang bergantung pada data dan informasi digital. Oleh karena itu keamanan memiliki peran penting dalam menjaga data dan

informasi penting milik perusahaan. Dalam mengamankan sebuah data dibutuhkan suatu keamanan yang dapat mencegah hilangnya data dan informasi penting perusahaan. [1] Salah satu contoh keamanan yang dapat digunakan untuk menjaga data dan informasi perusahaan adalah keamanan data. Dalam keamanan data salah satu metode yang dapat digunakan adalah metode enkripsi Algoritma AES (*Advanced Encryption Standard*).

Penelitian sebelumnya yang hampir serupa pernah dilakukan oleh Rifkie Primartha dari Universitas Sriwijaya dalam penelitiannya memadukan algoritma kriptografi AES dan kehandalan Bahasa pemrograman java untuk membuat suatu aplikasi perangkat lunak yang dapat melakukan fungsi kriptografi. [2]

Penelitian yang akan dibangun berdasarkan permasalahan yang ada maka peneliti akan membangun sebuah sistem keamanan data untuk mengatasi permasalahan kehilangan data yang ada pada PT. Baratim Info Bumi menggunakan metode algoritma AES (*Advanced Encryption Standard*). Cara kerja metode algoritma AES (*Advanced Encryption Standard*) ini untuk menjaga sebuah data yang bersifat rahasia tidak dapat diketahui oleh orang yang tidak bertanggung jawab. Dalam sistem ini dilengkapi juga dengan metode Hash Function, Hash Function yang digunakan yaitu *SHA-256* metode ini mampu mengamankan keaslian file yang dimana metode ini mampu merubah nama asli file menjadi nama acak yang telah dienkripsi. Sistem ini berguna untuk admin dan karyawan yang ada pada PT. Baratim Info Bumi dalam berbagi sebuah data.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang ada pada latar belakang maka ada beberapa masalah yang akan dibahas pada penelitian ini :

1. Bagaimana cara kerja algoritma AES (*Advanced Encryption Standard*) dalam sistem keamanan data?
2. Bagaimana cara kerja *Hash SHA-256* dalam sistem keamanan data?
3. Bagaimana cara agar berbagi file menjadi lebih aman?
4. Bagaimana cara enkripsi data menggunakan AES (*Advanced Encryption Standard*) dalam mengamankan sebuah data?

5. Bagaimana dekripsi data menggunakan AES (*Advanced Encryption Standard*) ?

1.3 Maksud Dan Tujuan

1.3.1 Maksud

Maksud dari penelitian ini adalah menerapkan metode Enkripsi Algoritma AES (*Advanced Encryption Standard*) dan Hash SHA-256 pada sistem keamanan data untuk meminimalisir ancaman kehilangan data penting yang ada pada PT. Baratim Info Bumi.

1.3.2 Tujuan

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

1. Menerapkan metode keamanan data Enkripsi AES (*Advanced Encryption Standard*).
2. Menerapkan metode keamanan data *Hash SHA-256*.
3. Meminimalisir kehilangan data penting yang disebabkan oleh orang yang tidak bertanggung jawab.
4. Membuat pengguna menjadi lebih aman ketika berbagi informasi dan data.
5. Membungkus data dengan sebuah enkripsi.

1.4 Batasan Masalah

Pada pengerjaan penelitian ini memiliki ruang lingkup yang sangat luas, maka batasan masalah yang digunakan pada penelitian ini adalah sebagai berikut :

1. Tempat penelitian dilakukan pada PT. Baratim Info Bumi.
2. Sistem yang dibangun berbasis website.
3. Sistem yang dibangun hanya untuk ruang lingkup PT. Baratim Info Bumi.
4. Data pendukung didapatkan dari PT. Baratim Info Bumi.
5. File yang dapat dilakukan enkripsi merupakan file ArcGIS.
6. Algoritma AES yang digunakan yaitu AES (*Advanced Encryption Standard*) 128 bit.
7. *Hash Function* yang digunakan yaitu *Hash SHA-256*.

8. AES (*Advanced Encryption Standard*) 128 bit digunakan untuk melakukan enkripsi terhadap file ArcGIS.
9. *Hash SHA-256* digunakan untuk melakukan enkripsi terhadap nama asli file dan password file yang akan dilakukan enkripsi.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan penelitian kualitatif, penelitian kualitatif adalah penelitian yang bersifat deskriptif dan cenderung menggunakan analisis. Proses dan makna (perspektif subjek) lebih ditonjolkan dalam penelitian kualitatif. Landasan teori dimanfaatkan sebagai pemandu agar fokus penelitian sesuai dengan fakta di lapangan.

1.5.1 Metode Pengumpulan Data

1. Studi Literatur

Studi literatur utama pada penelitian ini bersumber dari beberapa jurnal, buku, paper dan sumber bacaan yang dapat mendukung topik penelitian yang sedang dilakukan.

2. Wawancara

Metode wawancara ini digunakan untuk mengetahui masalah apa yang terjadi pada perusahaan dan agar mengetahui solusi yang diinginkan terhadap masalah yang ada pada perusahaan.

3. Observasi

Teknik pengumpulan data observasi dilakukan dengan mengamati langsung terhadap objek yang diteliti. Teknik observasi pada penelitian ini dilakukan untuk mengumpulkan data pengujian pada aspek performance efficiency, compatibility, dan reliability.

1.5.2 Metode Pembangunan Perangkat Lunak

Metode pembangunan perangkat lunak yang digunakan adalah menggunakan metode sekuensial linier (waterfall). Pressman (2001), metode Waterfall adalah suatu proses pengembangan perangkat lunak berurutan, di mana kemajuan dipandang sebagai terus mengalir ke bawah (seperti air terjun) melewati

fase-fase perencanaan, pemodelan, implementasi (konstruksi), dan pengujian. [3]
Berikut adalah Waterfall Development Model :

1. Rekayasa dan pemodelan sistem/informasi

Langkah pertama dimulai dengan membangun keseluruhan elemen sistem dan memilah bagian-bagian mana yang akan dijadikan bahan pengembangan perangkat lunak, dengan memperhatikan hubungannya dengan Hardware, User, dan Database.

2. Analisis kebutuhan perangkat lunak

Pada proses ini, dilakukan penganalisaan dan pengumpulan kebutuhan sistem yang meliputi Domain informasi, fungsi yang dibutuhkan unjuk kerja/performansi dan antarmuka. Hasil penganalisaan dan pengumpulan tersebut didokumentasikan dan diperlihatkan kembali kepada pelanggan.

3. Desain Sistem

Pada proses Desain, dilakukan penerjemahan syarat kebutuhan sebuah perancangan perangkat lunak yang dapat diperkirakan sebelum dibuatnya proses pengkodean (coding). Proses ini berfokus pada struktur data, arsitektur perangkat lunak, representasi interface, dan detail algoritma prosedural.

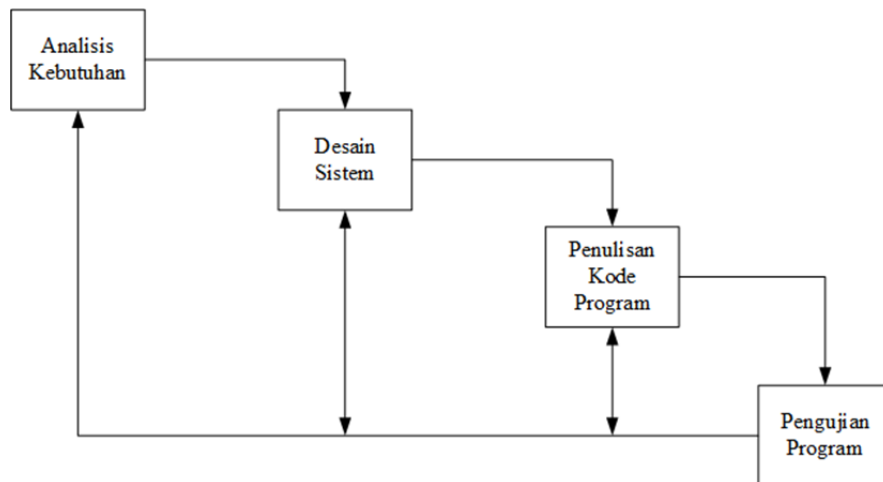
4. Penulisan Kode Program

Pengkodean merupakan proses menterjemahkan perancangan desain ke bentuk yang dapat dimengerti oleh mesin, dengan menggunakan bahasa pemrograman.

5. Pengujian Program

Setelah Proses Pengkodean selesai, dilanjutkan dengan proses pengujian pada program perangkat lunak, baik Pengujian logika internal, maupun Pengujian eksternal fungsional untuk memeriksa segala kemungkinan terjadinya kesalahan dan memeriksa apakah hasil dari pengembangan tersebut sesuai dengan hasil yang diinginkan.

Adapun tahapan model waterfall dapat dilihat pada gambar 1 Waterfall:



Gambar 1.1 Waterfall Model

1.6 Sistematika Penulisan

Sistematika penulisan penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan penelitian ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Dalam bab ini diuraikan mengenai latar belakang masalah, identifikasi masalah, maksud dan tujuan penelitian, batasan masalah, metode penelitian, deskripsi umum sistem, review literatur, jadwal dan tempat penelitian dan sistematika penelitian.

BAB 2 TINJAUAN PUSTAKA

Bab ini menguraikan tentang teori yang berhubungan dengan judul penelitian.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi tentang pembahasan deskripsi sistem, analisis kebutuhan dalam pembangunan sistem serta perancangan.

BAB 4 IMPLEMENTASI SISTEM DAN PENGUJIAN

Bab ini berisi tentang tahapan-tahapan yang dilakukan untuk menerapkan sistem yang telah dirancang. implementasi sistem yang berisi source code dan print screen tampilan dari sistem yang dibangun serta pengujian sistem yang dibangun.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan yang merupakan ringkasan bab-bab sebelumnya dan saran-saran berisi tentang tindak lanjut atau pengembangan yang dapat dilakukan terhadap sistem yang telah dibuat.