BAB 1
PENDAHULUAN

1.1 Latar Belakang

Puslitbang Geologi Kelautan merupakan Pusat Penelitian dan Pengembangan Geologi Kelautan yang di kelola instansi pemerintah di bawah departemen ESDM. Pada awalnya, PPGL didukung oleh empat bidang teknis, yaitu: Bidang Geologi Kelautan, Bidang Geofisika Kelautan, Bidang Sarana Operasi Kelautan, Bidang Manajemen Informasi dan Bagian Umum, dengan jumlah sumber daya manusia 222 orang. Sarana dan prasarana yang dimiliki sebagian berasal dari P3G [1].

Perpustakaan digital di Pulitbang salah satunya bagian sarana pelayanan publik yang berada di tempat instansi perusahaan puslitbang geologi kelautan khususnya pengarsipan, proses pengarsipan dilakukan secara manual/konvensional, misalnya dengan menyimpan laporan-laporan dalam sebuah map yang kemudian disimpan di dalam lemari arsip. Tentunya cara seperti ini tidak efektif dan efisien karena semakin banyak laporan yang akan diarsipkan maka akan semakin besar juga ruang yang dibutuhkan untuk menyimpan arsip tersebut.

Pada saat ini di P3GL menghadapi masalah dalam keamanan laporan, laporan bebas diakses oleh berbagai pihak dan tidak ada pengamanan dalam laporan laporan antara lain laporan penelitian, pemetaan, inventaris, dan penyelidikan sehingga orang bisa membaca dan merubah karna belum ada aplikasi untuk mengenkripsi file, maka dari itu diperlukan suatu keamanan yang baik sehingga laporan yang terdapat pada komputer menjadi lebih aman.

Berdasarkan permasalahan yang ada maka diperlukan sebuah aplikasi untuk mengamankan laporan pengarsipan di instansi P3GL tersebut. Dalam hal ini khususnya untuk membatasi pihak lain untuk melihat laporan agar mengurangi penggunaan tanpa izin oleh P3GL. Salah satu caranya adalah membuat data informasi tersebut tidak terbaca / tidak dapat dimengerti oleh pihak lain. Untuk hal itu penelitian kali ini akan menggunakan pengamanan dengan teknik kriptografi yang dapat

membuat data informasi digital tidak terbaca menggunakan algoritma Advanced Encryption Standard (AES).

Dengan demikian maka penelitian ini akan berfokus untuk membangun aplikasi keamanan sistem yang berjudul "Implementasi Algoritma Advanced Encryption Standard (AES) Sebagai Sistem Pengamanan Data Pengarsipan Pada Perpustakaan Digital di Puslitbang Geologi Kelautan".

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang masalah diatas, masalah-masalah yang ada dapat diidentifikasi sebagai berikut:

1. Belum ada pembatasan hak akses untuk melihat pengarsipan data digital.
2. Bagaimana menerapkan algoritma Advanced Encryption Standard (AES) dalam pengenkripsian data rahasia sehingga data yang telah dienkripsi tidak dapat dibaca atau dimengerti oleh pihak lain.

1.3 Maksud dan Tujuan Penelitian

Maksud dari penulisan tugas akhir ini adalah menerapkan algoritma advanced encryption standard (AES) sebagai sistem pengamanan data pengarsipan pada perpustakaan digital.

Sedangkan tujuan yang akan dicapai pada penelitian yang akan dilakukan adalah sebagai berikut:

1. Membuat pembatasan hak akses untuk melihat pengarsipan data digital.
2. Membuat sebuah aplikasi yang dapat melakukan enkripsi dan dekripsi data dengan menggunakan algoritma Advanced Encryption Standard yang akan digunakan untuk mengamankan data penting sebuah instansi pemerintahan di Puslitbang Geologi Kelautan.

1.4 Batasan Masalah

Dalam penelitian ini ditetapkan beberap batasan masalah, diantaranya sebagai berikut:

1. Format Laporan yang bisa dilakukan enkripsi yaitu .pdf
2. Sebelum data disembunyikan terlebih dahulu dilakukan penyandian dengan password yang dikonversi menjadi byte menggunakan SHA-1 kemudian file dienkripsi menggunakan algoritma AES (Advance Encryption Standard) 128 bit
3. Proses otentikasi password menggunakan fungsi hash SHA-1.
4. Sistem ini akan menghasilkan sebuah chipertext dengan format file .pdf

Sistem berbasis *website*. Menggunakan PHP, Html dan *library* pembuatan web lainnya.

1.5 Metodelogi Penelitian

Metode penelitian akan menggunakan metode kualitatif. Metode penelitian kualitatif merupakan suatu metode yang penelitian yang bermaksud untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian misalnya perilaku, persepsi, motivasi, tindakan dan lain sebagainya.

Secara singkat dapat dijabarkan bahwa metode penelitian kualitatif merupakan metode yang didasarkan pada kasus khusus sehingga pengumpulan dan analisis data bersifat khusus pula.

Karena sifatnya yang bersifat khusus itu maka metode penelitian kualitatif sering digunakan dalam berbagai *research*, meskipun beberapa kalangan menolak metode ini karena dianggap tidak bisa mewakili sifat umum penelitian. Namun metode ini tetap saja digemari karena pada prinsipnya bahwa teori yang berkembang perlu menyesuaikan dengan keadaan lingkungannya

.

1.6 Metode Pengumpulan Data

Metode pengumpulan data yang akan digunakan berdasar metode yang digunakan maka diperoleh beberapa teknik pengumpulan data sebagai berikut :

1. Metode Penelitian (Observasi)

   Dengan metode observasi penulis mendapatkan data dengan cara mendatangi langsung instansi yang dijadikan tempat riset.

2. Metode Wawancara (Interview)

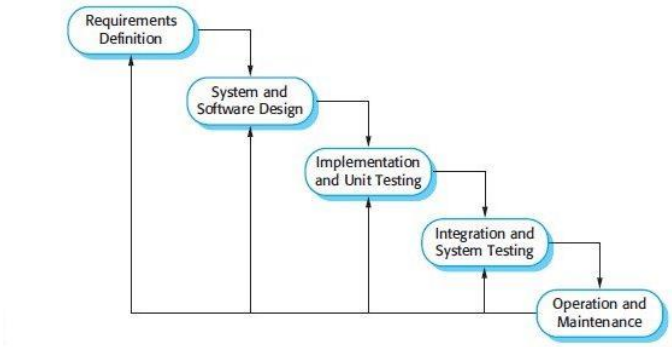
   Interview yang berupa tanya jawab penulis lakukan kepada beberapa staff yang terkait langsung dengan instansi, interview dilakukan kepada staff bagian affiliasi.

3. Metode Study Pustaka (Library Search)

   Metode ini dilakukan guna mendapatkan gambaran secara teoritis yang berkaitan dengan penulisan laporan penelitian sebagai acuan. Penulis mengumpulkan data yang bersumber dari materi yang didapat semasa kuliah, seperti modul pemrograman PHP, berbagai buku panduan dalam mengerjakan laporan penelitian, contoh laporan-laporan terdahulu yang dibuat oleh para mahasiswa yang sudah melakukan penelitian.

1.7 Metode Pembangunan Perangkat Lunak

Metode analisis data dalam pembuatan perangkat lunak menggunakan meode waterfall. Berikut ini akan dijelaskan mengenai tahap-tahap pembangunan sistem dengan menggunakan metode waterfall.



Gambar 1.1 Metode *Waterfall*

Keterkaitan dan pengaruh antar tahap ini ada karena output sebuah tahap dalam Waterfall Model merupakan input bagi tahap berikutnya, dengan demikian ketidaksempurnaan hasil pelaksanaan tahap sebelumnya adalah awal ketidaksempurnaan tahap berikutnya. Berikut adalah penjelasan detail dari masing-masing tahap dalam waterfall model, yaitu:

1. *Requirements analysis and definition*
   Tahap ini merupakan bagian dari kegiatan sistem yang terbesar dalam pengerjaan suatu proyek. Pada tahap ini merupakan tahap pertama yang menjadi dasar proses pembuatan perangkat lunak.
2. *System and software design*
   Tahap menerjemahkan kebutuhan-kebutuhan yang dianalisis ke dalam bentuk yang mudah dimengerti. Sehingga didapat jelas fungsi dan kebutuhan yang diinginkan dari pembangunan atau pengembangan perangkat lunak tersebut.
3. *Implementation and unit testing*
   Tahap penerjemahan data atau pemecahan masalah yang telah dirancang kedalam suatu bahasa pemrograman tertentu. Setiap fungsional yang ada pada perangkat lunak tersebut dilakukan uji kelayakan, sehingga perangkat lunak tersebut dapat berjalan dengan baik.
4. *Integration and System Testing*
   Pada tahap ini, dilakukan penyempurnaan terhadap perangkat lunak secara keseluruhan agar dapat berjalan sesuai dengan kebutuhan. Pengujian perangkat lunak terhadap data nyata perlu dilakukan untuk memastikan kelayakan dari perangkat lunak tersebut.
5. *Operation and Maintenance*
   Tahap akhir dimana suatu perangkat lunak yang sudah selesai dapat dioperasikan langsung oleh pengguna. Tahap maintenance perlu dilakukan untuk disesuaikan apabila ada perubahan sesuai dengan permintaan pengguna.

1.8 Sistematika Penulisan

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

BAB 1 PENDAHULUAN

Pada bab pendahuluan ini, penulis menguraikan tentang secara singkat tentang latar belakang masalah, rumusan masalah, maksud dan tujuan disusunnya penulisan skripsi ini serta batasan-batasan yang digunakan untuk menyelesaikan penulisan skripsi ini. Serta menguraikan pula tentang metodologi penelitian yang digunakan serta sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Pada bab ini, berisi penjelasan seperti profil, sejarah, tujuan, visi dan misi instansi P3GL. Serta membahas teori-teori yang berkaitan dengan judul dari penulisan skripsi ini.

BAB 3 ANALISIS DAN PERANCANGAN

Berisi analisis kebutuhan untuk sistem yang akan dibangun sesuai dengan metode pengembangan perangkat lunak yang digunakan. Selain itu, bab ini juga berisi perancangan struktur antar muka untuk sistem yang akan dibangun sesuai analisis yang telah dilakukan.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi implementasi dari hasil analisis dan perancangan algoritma Advanced Encryption Standard (AES) sebagai sistem pengamanan data pengarsipan pada perpustakaan digital yang telah dibuat, disertai juga dengan hasil pengujian dari aplikasi kriptografi dengan menggunakan algoritma Advanced Encryption Standard (AES) pada pengamanan data pengarsipan digital sehingga diketahui apakah aplikasi yang dibangun dapat bermanfaat untuk mengamankan data pengarsipan digital.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari penelitian yang dilakukan dan juga berisikan tentang saran yang nantinya diperlukan untuk penelitian lebih lanjut.