BAB I

PENDAHULUAN

I.1. Latar Belakang

Google Drive adalah layanan penyimpanan daring milik *Google* yang diluncurkan pada 24 April 2012. Layanan ini merupakan ekstensi dari *Google* Docs dan akan mengganti URL docs.*google*.com dengan *drive*.*google*.com setelah diaktifkan. *Google Drive* memberikan layanan penyimpanan gratis sebesar 15 GB dan dapat ditambahkan dengan pembayaran tertentu. Dengan fitur unggulan yang sama seperti *Dropbox*, yaitu sinkronisasi data melalui folder khusus di dalam desktop atau lebih dikenal dengan *Desktop Sync Clients*. *GDrive* memberikan kapasitas gratis sebesar 5 GB dan tentunya fitur-fitur yang terintegrasi dengan layanan *Google* lainnya seperti: Gmail, G+ dan *Google Search*. Fitur yang bisa digaris bawahi dari G*Drive* adalah API's untuk para Developer. Hingga kini G*Drive* telah terhubung dengan puluhan aplikasi pihak ketiga.

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi jika data tersebut berada dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan lain. Hal tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Yang mana jika hal Tersebut sampai terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang mengirim pesan atau menerima pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah

sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang dibajak tersebut akan memiliki kemungkinan rusak bahkan hilang yang akan menimbulkan kerugian material yang besar.

Adapun kelebihan dari perancangan aplikasi ini adalah aplikasi *google drive* dengan memanfaatkan sistem keamanan data dapat menjaga kerahasiaan dan keamanan pengiriman data pada aplikasi *google drive* sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer data atau pesan dan implementasi Kriptografi TEA (*Tiny Encryption Algorithm*) terhadap aplikasi *google drive* dapat memberikan refrensi baru terhadap peneliti selanjutnya mengenai metode keamanan data.

Tiny Encryption Algorithm (TEA) merupakan suatu algoritma sandi yang diciptakan oleh David J. Wheeler dan Roger M. Needham dari Cambridge University tahun 1994. Algoritma ini merupakan algoritma penyandian block cipher yang dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal. Sistem penyandian TEA menggunakan proses feistel network dengan menambahkan fungsi matematik berupa penambahan dan pengurangan sebagai operator pembalik selain XOR. Hal ini dimaksudkan untuk menciptakan sifat non-linearitas. Pergeseran dua arah (ke kiri dan ke kanan) menyebabkan semua bit kunci dan data bercampur secara berulang ulang (Mukti Qamal ; 2014 : 21).

Alasan penulis mengambil judul penelitian "**Perancangan Aplikasi Pengamanan Data Pada *Google Drive* Dengan Menggunakan Algoritma TEA**" karena tidak adanya implementasi kriptografi TEA dalam pengembangan aplikasi Pengamanan Data Pada *Google Drive*.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Permasalahan yang ada pada penelitian ini adalah :

1. Tidak adanya sistem keamanan data yang aman pada penyimpanan data di *google drive*.
2. Belum berkembangnya algoritma Kriptografi TEA (*Tiny Encryption Algorithm*) dalam sistem keamanan *google drive*.

I.2.2. Perumusan Masalah

Perumusan masalah yang ada pada penelitian ini yaitu:

1. Bagaimana merancang sebuah aplikasi yang memiliki sistem keamanan data yang aman pada penyimpanan data di *google drive* ?
2. Bagaimana melakukan perkembangan algoritma Kriptografi TEA (*Tiny Encryption Algorithm*) dalam sistem keamanan *google drive* ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

1. Data yang dibutuhkan dalam melakukan perancangan sistem adalah *file plain, file encrypted, password, api key google, api secret google.*
2. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *javascript, netbeans 8.0.*

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan penelitian ini yaitu:

1. Merancang sebuah aplikasi *google drive* dengan memanfaatkan sistem keamanan data yang dapat menjaga kerahasiaan dan keamanan pengiriman data pada aplikasi *google drive*.
2. Merancang dan membangun sebuah aplikasi *google drive* dengan menggunakan Kriptografi TEA (*Tiny Encryption Algorithm*).

I.3.2. Manfaat

Manfaat penelitian ini yaitu:

1. Aplikasi *google drive* dengan memanfaatkan sistem keamanan data dapat menjaga kerahasiaan dan keamanan pengiriman data pada aplikasi *google drive* sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer data atau pesan.
2. Implementasi Kriptografi TEA (*Tiny Encryption Algorithm*) terhadap aplikasi *google drive* dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal.

I.4. Metodologi Penelitian

I.4.1. Metode Penelitian

Metode penelitian yang dipakai oleh penulis adalah metode penelitian deskriptif atau disebut juga metode penelitian analitis. Dalam metode penelitian deskriptif ini digunakan teknik-teknik analisis, klasifikasi masalah, survei, studi kepustakaan terhadap masalah-masalah yang berhubungan dengan skripsi yang penulis susun, wawancara (*interview*) dengan narasumber, observasi, dan teknik *Test* terhadap objek penelitian yang telah ada.

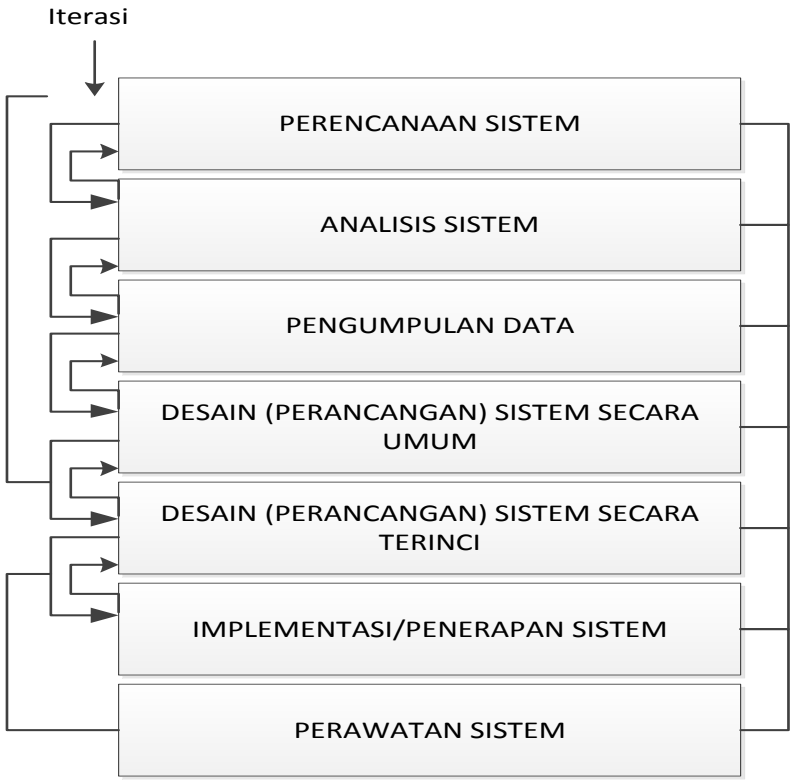
Penulis menggunakan metode penelitian deskriptif dikarenakan pemecahan masalah yang aktual yaitu masalah yang berkembang pada bidang *artifisial intelligence* yang sekarang sedang berkembang pesat. Dengan metode deskriptif, aplikasi yang telah penulis kumpulkan mula-mula disusun, dijelaskan, dianalisis, dan kemudian diimplementasikan dalam sebuah perangkat lunak.

I.4.2. Metode Pengembangan Perangkat Lunak

Metodologi atau teknik yang digunakan dalam pengembangan dan pembuatan perangkat lunak meliputi metodologi konvensional (sebelum pertengahan 1970-an), struktural klasik (mulai pertengahan 1970-an), struktural modern (mulai pertengahan 1980-an) dan *post modern* (mulai akhir 1980-an).

Metodologi pengembangan perangkat lunak yang penulis gunakan adalah *post modern* yang populer digunakan mulai akhir 1980-an. Metodologi ini mencirikan adanya paradigma *objectoriented* dan multimedia. Beberapa *tool* yang bisa digunakan sebagai alat pengembangan dan pembuatan program yang berorientasi objek (*Object Oriented Programming*).

Pengembangan sistem dapat berupa menyusun suatu sistem yang baru dan menggantikan sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada. Setiap tahap harus diselesaikan terlebih dahulu kemudian diteruskan ketahap berikutnywa untuk menghindari terjadinya pengulangan tahap. Metodologi pengembangan sistem *Waterfall* dapat dilihat di bawah ini :



Gambar I.1 Struktur Pengembangan Sistem

Dari gambar diatas dapat dijelaskan sebagai berikut :

1. Perencanaan sistem

   Manfaat dari tahapan ini adalah untuk menentukan masalah-masalah atau kebutuhan yang timbul. Hal ini memerlukan pengembangan sistem secara menyeluruh agar ada usaha lain yang dapat di lakukan untuk memecahkan masalah tersebut. Adapun masalah yang timbul adalah :

   a. Tidak adanya sistem keamanan data yang aman pada penyimpanan data di google drive.

b. Belum berkembangnya algoritma Kriptografi TEA (*Tiny Encryption Algorithm*) dalam sistem keamanan google drive

2. Analisa Sistem.

   Tahap analisa bertitik tolak pada kegiatan-kegiatan dan tugas-tugas dimana sistem yang berjalan di pelajari lebih mendalam, konsepsi dan usulan dibuat untuk menjadi landasan bagi sistem yang baru yang akan dibangun.

   a. Data yang dibutuhkan dalam melakukan perancangan sistem adalah *file plain, file encrypted, password, api key google, api secret google.*
   b. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *javascript, netbeans 8.0*.

3. Pengumpulan Data

   Pengumpulan data adalah cara-cara yang dapat digunakan oleh peneliti untuk mengumpulkan data. Instumen sebagi alat bantu dalam menggunakan methode pengumpulan data merupakan sarana yang dapat diwujudkan dalam benda, misalnya angket, perangkat tes, pedoman wawancara, pedoman observasi, skala dan sebaginya.

4. Desain (Perancangan) Sistem Secara Umum.

   Pada tahap ini akan membahas mengenai desain sistem yang digunakan oleh penulis, membahas mengenai aplikasi-aplikasi yang digunakan dalam pembuatan desain program.

   a. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *javascript, netbeans 8.0*.
   b. *Appserv*, sebagai paket software untuk menjalankan DBMS *MySQL 5*
   c. PC dengan *Processor* IV 1,6 Ghz, Memori 512MB, Kartu Grafik 512 MB

5. Desain (Perancangan) Sistem Secara Terinci

Pada tahap ini sebagian besar kegiatan yang berorientasi ke komputer dilaksanakan. Spesifikasi perangkat keras dan perangkat lunak yang telah disusun pada tahap sebelumnya ditinjau kembali dan disempurnakan. Rencana pembutan program dilaksakan dan juga testing programnya. Testing program menggunakan metode *blackbox testing*. *Black box testing* adalah pengujian yang dilakukan hanya mengamati hasil eksekusi melalui data uji dan memeriksa fungsional dari perangkat lunak. Jadi dianalogikan seperti kita melihat suatu koatak hitam, kit hanya bisa melihat penampilan luarnya saja, tanpa tau ada apa dibalik bungkus hitam nya. Sama seperti pengujian black box, mengevaluasi hanya dari tampilan luarnya (interface nya), fungsionalitasnya.tanpa mengetahui apa sesungguhnya yang terjadi dalam proses detilnya (hanya mengetahui *input* dan *output*).

6. Implementasi Sistem

   Perancangan sistem pakar identifikasi penyakit alzeimer yang telah dirancang oleh penulis membutuhkan implementasi metode untuk menyempurnakan keamanan data, metode yang digunakan oleh penelitian adalah *Tiny Encryption Algorithm* (TEA)

7. Pemeliharaan Sistem

Tujuan tahapan ini adalah untuk melakukan evaluasi sistem secara tepat dan efisien, menyempurnakan proses pemeliharaan sistem dengan selalu menganalisa kebutuhan informasi yang dihasilkan sistem tersebut.

I.6. Keaslian Penelitian

Berikut adalah beberapa jurnal penelitian terdahulu terkait judul penelitian skripsi ini pada tabel I.1 :

Tabel I.1. Keaslian Penelitian

No	Peneliti	Judul	Hasil
1	Mukti Qamal (2014)	Kriptografi File Citra Menggunakan TEA (*Tiny Encryption Algorithm*)	Pertumbuhan tajam komunikasi data baru-baru ini meningkatkan pentingnya keamanan data dan kerahasiaan. Kriptografi adalah seni atau ilmu menjaga keamanan data atau pesan yang mengacak data atau pesan. Selain dokumen berbasis teks, juga umum untuk mengirim gambar melalui jaringan. Penelitian ini menyelidiki cara untuk mengamankan gambar dari gangguan cryptanalyst dengan menggunakan TEA (kecil Encryption Algorithm) algorith, yang merupakan kunci algoritma kriptografi rahasia. Kekuatan algoritma ini terletak pada Feistel jaringan dan jumlah delta berasal dari jumlah emas. Ditemukan bahwa algoritma yang sesuai untuk mengenkripsi dan mendekripsi gambar, karena putaran kuat kuantitas dan panjang kunci, dan tidak perlu S-box dan P-box dalam proses. tes menunjukkan bahwa algoritma ini dengan 32 putaran cocok sangat untuk mengamankan gambar dengan kecepatan optimal. Dulu juga menemukan bahwa ukuran gambar yang lebih besar, semakin lama proses enkripsi dan dekripsi membutuhkan waktu untuk menjalankan, dengan gambar didekripsi memiliki berbagai nilai kedalaman bit dibandingkan dengan gambar asli
2	Khandar William (2014	Studi mengenai *Tiny Encryption Algorithm* (TEA) dan turunan-turunannya (XTEA dan XXTEA)	Roger M. Needham dan David J. Wheeler menciptakan *Tiny Encryption Algorithm* (TEA), XTEA, dan XXTEA yang terkenal dengan kesederhanaan implementasinya. Pertama mereka menciptakan TEA, lalu kelemahan dari TEA ditutupi oleh XTEA, setelah itu mereka juga menciptakan Block TEA, yaitu algoritma XTEA yang dimodifikasi untuk dapat menerima blok

			sebesar apapun, dan terakhir mereka menciptakan XXTEA yang menutupi kelemahan dari Block TEA. Makalah ini akan membahas secara mendalam mengenai TEA, XTEA, dan XXTEA. Makalah ini juga membahas kelehaman dari TEA dan Block TEA yang mengakibatkan munculnya XTEA dan XXTEA. Selain itu, makalah ini juga membahas serangan-serangan yang mengekspoitasi kelemahan-kelemahan tersebut.
3	Rini Khorianti (2014)	Implementasi Algoritma TEA Untuk Enkripsi dan Dekripsi Menggunakan Bahasa Pemrograman Visual Basic	Keamanan data merupakan salah satu aspek terpenting dalam teknologi informasi. Dengan tingkat keamanan yang tinggi, diharapkan informasi yang disajikan dapat terjaga keasliannya. Sistem ini dibangun menggunakan bahasa pemrograman *Visual Basic*. *Visual basic* adalah pemrograman berbasis Windows, dimana dalam tingkat dasar untuk melakukan pemrograman visual basic cukup sederhana yaitu dengan mengatur menu, dan menggunakan bahasa Inggris sederhana sebagai bahasa pemrogramannya. Algoritma TEA *(Tiny Encription Algorithm)* digunakan sebagai kunci rahasia. Hasil dari proses *enkripsi* adalah *ciperteks* yang berukuran 16 *byte* atau kelipatannya. Algoritma kriptografi TEA lebih aman dikarenakan jumlah *round* serta panjang kuncinya yang lebih panjang

I.7. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi yaitu berupa pembahasan mengenai sistem jaringan, UML, ERD dan normalisasi.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.