BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

PT Infokes Indonesia yang berfokus pada pengembangan produk dan solusi teknologi informasi kesehatan online dan terpadu di Indonesia telah menghasilkan beberapa produk di antaranya yaitu ePuskesmas, eHospital, eClinic, dan lain-lain. Pada PT Infokes arsip *database* klien disimpan dalam media penyimpanan sekunder. Selain itu transaksi *database* dengan klien dilakukan secara konvensional, yaitu dengan mengirimkan *database* yang sudah tersimpan di dalam media penyimpanan sekunder melalui kurir ekspedisi. Hal tersebut menyebabkan *database* dapat dibaca dengan mudah oleh orang lain dan dikhawatirkan menjadi celah kebocoran informasi yang bersifat privasi dan rahasia kepada publik. Meskipun belum pernah ada kasus di PT Infokes namun kebocoran informasi tersebut pernah terjadi, misalnya pada PT Pindad [1] dan Polsek Mangkubumi [2].

Teknik kriptografi merupakan salah satu alternatif solusi yang dapat digunakan dalam pengamanan informasi [1] [2] [3] [4] . Teknik kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas [5]. Komponen di dalam kriptografi untuk menjaga keamanan *database* tersebut adalah menggunakan teknik enkripsi. Ada berbagai macam teknik enkripsi dalam kriptografi, salah satunya model enkripsi RC4. Model enkripsi RC4 memiliki kelebihan dalam kecepatan pemrosesan data [6] bahkan mencapai 10 kali lebih cepat dari DES [7, 6]. Algoritma *stream cipher* RC4 memiliki tingkat efisiensi yang baik dalam penyimpanan data pada *database,* karena hasil enkripsi yang dihasilkan sama jumlahnya dengan karakter aslinya [8]. Selain itu, jika masukkan yang akan dienkripsi mengandung kata berulang maka akan menghasilkan *ciphertext* yang acak. Masukkan yang berulang hasilnya tidak sama dengan masukkan yang sebelumnya karena setiap karakter dari *plaintext* di XORkan dengan kunci yang dibangkitkan [9]. Meskipun demikian, algoritma RC4 memiliki kerentanan terhadap *Bit Flipping Attack*. *Bit Flipping Attack* atau BFA adalah serangan pada algoritma *stream cipher* dengan

tujuan untuk mengubah hasil enkripsi dengan cara mengubah *bit ciphertext* tertentu yang tentu saja dapat menurunkan performa kinerja RC4 sebagai metode enkripsi [10]. RC4 juga rentan terhadap *cryptanalysis* yang dapat membaca pesan asli atau *plaintext* dengan melakukan analisis terhadap kunci yang mungkin digunakan [11].

Untuk meningkatkan keamanan diperlukan adanya kombinasi algoritma sehingga sulit dipecahkan. Dalam penelitian lain, sistem keamanan menggunakan algoritma kriptografi RC4 dan Base64 dapat menjamin keamanan karena data disamarkan dengan proses enkripsi dan sangat sulit dipecahkan apabila kunci dan perhitungan algoritma berbeda. Transformasi Base64 merupakan salah satu algoritma untuk *encoding* dan *decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyandian) terhadap data *binary* [4] [12]. *Encoding* dengan Base64 memberikan hasil berupa *plaintext*, sehingga data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa *binary* [3]. Namun dari penelitian yang sudah disebutkan sebelumnya, algoritma yang digunakan lebih efektif untuk mengenkripsi data berupa citra digital [1], sementara penelitian yang menggunakan data masukan berupa teks proses enkripsi maupun dekripsi dilakukan oleh sebuah algoritma saja [2] [8] [10] . Adapun penelitian lain yang menggunakan dua algoritma [4] baik kriptografi RC4 maupun Base64 hanya melakukan enkripsi sebagian data di dalam tabel tertentu.

Sehingga dalam penelitian ini penulis tertarik untuk mengambil judul, "Implementasi Algoritma Kombinasi RC4 dan Base64 untuk Mengamankan Database Klien PT Infokes". Dengan adanya kombinasi dua algoritma tersebut dapat menjadi salah satu teknik enkripsi yang cukup rumit sehingga apabila ada pihak yang bermaksud melihat *database* asli harus mengetahui kunci dan perhitungan algoritma yang digunakan.

1.2 Identifikasi Masalah

Identifikasi masalah yang terjadi adalah sebagai berikut:

1) Kurangnya tingkat keamanan pada arsip *database* PT Infokes karena belum terenkripsi.

2) Proses transaksi *database* dilakukan secara konvensional dan tanpa pengamanan.
3) Adanya kelemahan metode kriptografi RC4 yang rentan terhadap serangan *Bit Flipping Attack* dan memungkinkan dilakukannya *cryptanalysis*.

1.3 Maksud dan Tujuan

Maksud dari pelaksanaan penelitian ini adalah untuk membangun sistem keamanan data di PT Infokes. Sementara tujuannya adalah sebagai berikut:

1) Mengamankan *file* arsip *database* klien PT Infokes dengan kriptografi.
2) Mengamankan proses transaksi *database* dari Divisi Data dan Infrastruktur kepada klien PT Infokes.
3) Meningkatkan kinerja algoritma kriptografi RC4 dengan menambahkan kombinasi Base64.

1.4 Batasan Masalah

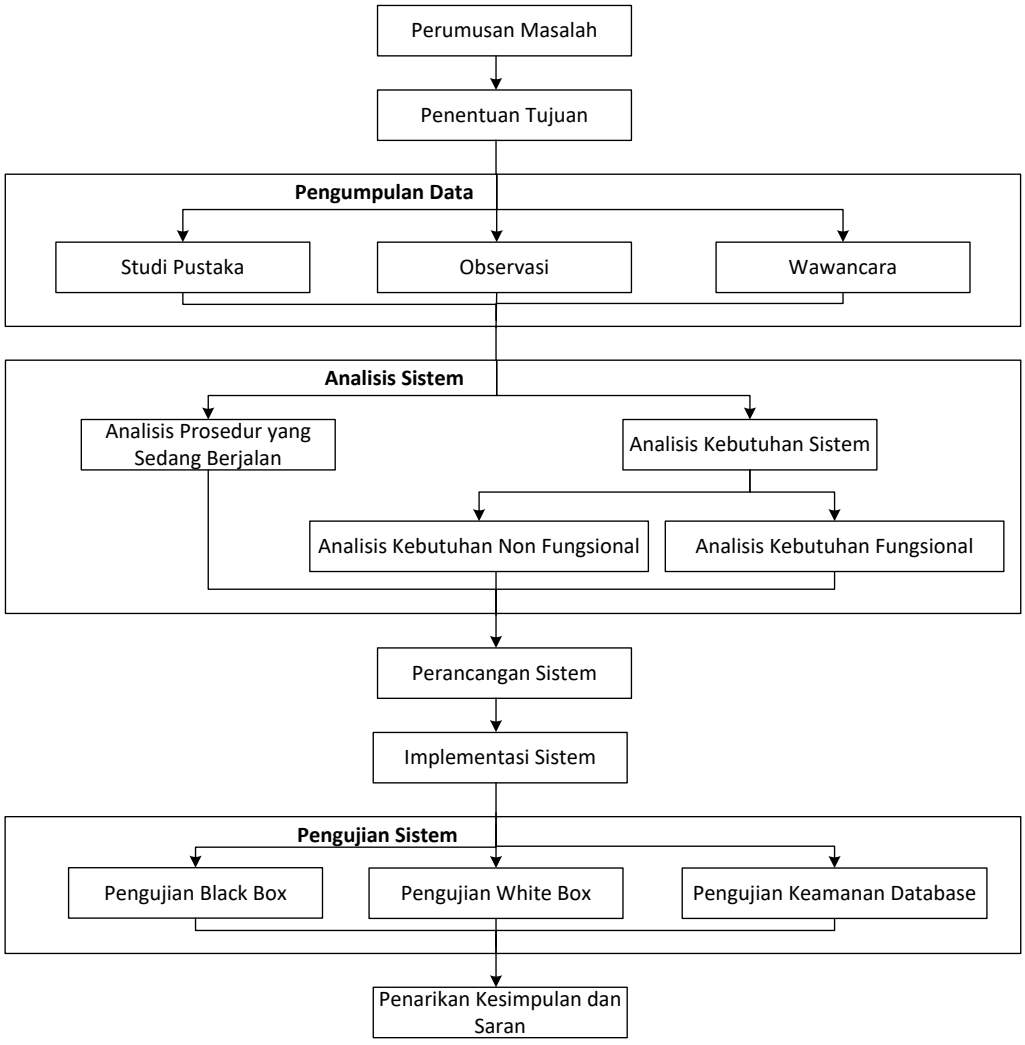
Adapun batasan masalah dalam penelitian ini adalah:

1) File yang akan dienkripsi berupa *database*.
2) Algoritma kriptografi yang digunakan adalah RC4 *stream cipher* yang dikombinasi dengan Base64.
3) Jenis kriptografi yang digunakan merupakan kriptografi simetris.
4) Sistem keamanan yang akan dibangun berbasis web dan menggunakan Bahasa Pemrograman PHP serta menggunakan protokol HTTPS.
5) Model proses data yang digunakan dalam pembangunan aplikasi adalah model OOP (Object Oriented Programming) dan pemodelan sistem menggunakan Unified Modelling Language (UML).
6) *Tools* yang digunakan untuk menguji keamanan *database* yaitu *CrypTool* versi1.4.41 dan *Wireshark* versi 3.0.3.
7) Sistem ini memiliki dua hak akses pengguna yaitu Divisi Data dan Infrastruktur dan klien PT Infokes.
8) Semua hasil enkripsi akan berekstensi .Ifk (diambil dari singkatan Infokes) dan dekripsi hanya bisa dilakukan untuk file yang berekstensi .Ifk

9) Satu kali enkripsi maupun dekripsi hanya dapat memproses satu file.

1.5 Metodologi Penelitian

Metodologi penelitian merupakan proses yang digunakan untuk memecahkan masalah secara logis. Adapun metodologi yang digunakan dalam penelitian ini menggunakan dua metode, yaitu metode pengumpulan data dan metode pembangunan perangkat lunak dengan model waterfall. Sedangkan untuk metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian terapan, yaitu penelitian yang berusaha mendeskripsikan suatu gejala, peristiwa, kejadian yang terjadi pada saat sekarang. Secara keseluruhan kerangka kerja yang diterapkan adalah sebagai berikut:



Gambar 1.1 Kerangka Kerja Penelitian

1) Perumusan Masalah

Pada tahap ini dilakukan peninjauan ke sistem yang akan diteliti untuk mengamati serta melakukan eksplorasi lebih dalam dan menggali permasalahan yang ada pada sistem yang berjalan saat ini. Tahap perumusan masalah, merupakan langkah awal dari penelitian ini, karena tahap ini diperlukan untuk mendefinisikan keinginan dari sistem yang tidak tercapai.

2) Penentuan Tujuan

Berdasarkan perumusan masalah yang telah dibuat pada tahap sebelumnya, maka tahap penentuan tujuan berguna untuk memperjelas kerangka tentang apa saja yang menjadi sasaran dari penelitian ini. Pada tahap ini ditentukan tujuan dari pembangunan sistem keamanan ini yaitu untuk meningkatkan keamanan data pada PT Infokes.

3) Pengumpulan Data

Pada tahap ini dilakukan pengumpulan data dan informasi untuk lebih mengetahui mengenai sistem yang diteliti. Dari data dan informasi yang dikumpulkan akan dapat diketahui mengenai sistem yang berjalan saat ini. Data-data dan informasi dapat diperoleh melalui wawancara dan pengamatan langsung. Adapun metode pengumpulan data yang dilakukan adalah dengan cara:

1. Observasi

Yaitu penelitian langsung di PT Infokes untuk mengetahui prosedur kerja yang sedang berjalan.

2. Wawancara

Pengumpulan data dengan proses tanya jawab langsung dan sistematis kepada narasumber (Kepala Divisi Data dan Infrastruktur PT Infokes) untuk mendapatkan data-data yang berkaitan dengan pengarsipan *database* maupun transaksi *database* dari Divisi Data dan Infrastruktur kepada klien.

3. Studi Pustaka

Pengumpulan data melalui buku-buku, dokumen, peraturan yang erat kaitannya dengan materi bahasan dalam sistem keamanan *database* di PT Infokes.

4) Analisis Sistem

Pada analisis sistem, akan dilakukan analisis prosedur yang berjalan saat ini secara tidak langsung akan terlihat kelemahan-kelemahannya, sehingga saat itu juga bisa dilakukan analisa kebutuhan sistem yang bertujuan untuk mengidentifikasikan hal apa saja yang masih kurang dari prosedur bisnis sebelumnya untuk kemudian dilakukan langkah-langkah perbaikan. Analisis kebutuhan sistem di sini dibagi menjadi dua yaitu analisis kebutuhan fungsional terkait arsitektur sistem dan analisis kebutuhan non fungsional terkait kebutuhan perangkat keras, kebutuhan perangkat lunak maupun pengguna.

5) Perancangan Sistem

Perancangan sistem dilakukan guna mendapatkan gambaran dengan jelas tentang apa yang dikerjakan pada analisa sistem dan dilanjutkan dengan mempertimbangkan bagaimana membentuk sistem tersebut.

6) Implementasi Sistem

Pada tahap ini akan dilakukan penerapan/implementasi sistem yang mengacu pada perancangan sistem yang telah dibuat. Pengimplementasian sistem memiliki kriteria mudah digunakan dan dipahami oleh pemakai.

7) Pengujian Sistem

Pengujian sistem yang telah dibangun bertujuan guna mengetahui kesesuaian program dengan analisa sistem yang telah dibuat hingga dapat dipakai. Ada tiga pengujian yang akan dilakukan yaitu Pengujian *Black box*, Pengujian *White box* dan Pengujian Keamanan *Database*.

8) Penarikan Kesimpulan dan Saran

Bagian ini berisi kesimpulan mengenai semua tahapan yang telah dilalui serta saran mengenai hasil dari penelitian yang telah dicapai.

1.6 Sistematika Penyusunan

Sistematika penyusunan proposal ini disusun untuk memberikan gambaran umum tentang kasus yang akan dipecahkan. Sistematika penyusunan laporan ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini membahas mengenai latar belakang, identifikasi masalah, maksud dan tujuan, manfaat, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menguraikan berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan di PT Infokes Indonesia.

BAB III ANALISIS DAN PERANCANGAN

Bab ini membahas tentang analisis deskripsi sistem, analisis perancangan fungsional, analisis kebutuhan non fungsional dan perancangan antarmuka dari perangkat lunak yang akan dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini berisikan implementasi antarmuka perangkat lunak, implementasi perangkat keras dan perangkat lunak, pengujian perangkat lunak (secara subjektif dan alpha) beserta kesimpulan dari hasil pengujian perangkat lunak yang dibangun.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang beberapa saran dan kesimpulan yang didapatkan dari hasil pembahasan bab-bab sebelumnya, serta saran-saran yang dapat dilakukan.