BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Keamanan dalam sistem informasi merupakan salah satu hal penting namun pemilik data atau pengelola sistem informasi sering kali mengabaikan atau tidak peduli terhadap aspek keamanan ini. Sehingga seseorang mudah melakukan pencurian, penyadapan atau mengubah informasi tanpa seizin pemilik data.

Pentingnya keamanan sebuah sistem informasi sangat diperlukan karena jika ada seseorang yang dapat mengakses sebuah sistem informasi tanpa adanya wewenang yang diberikan kepadanya, maka keakuratan informasi tersebut diragukan bahkan dapat menyesatkan[1].

Beberapa hal penting yang harus diperhatikan dalam sistem informasi web dan hal yang rentan terhadap penyerangan adalah manajemen akses. Umumnya akses database sebuah website terletak pada sistem otentikasi dan otorisasi pengguna. Otentikasi adalah proses menentukan validitas pengguna yang mengklaim dirinya sendiri sedangkan otorisasi adalah proses menentukan sumber daya apa yang diizinkan untuk diakses oleh pengguna.

Diantara penelitian yang telah dilakukan mengenai manajemen akses adalah pemanfaatan data kependudukan tingkat kabupaten menggunakan metode RBAC *(Role Back Access Control)* [2]. Model RBAC dalam penelitian tersebut hanya mengelompokan data berdasarkan atribut yang digunakan pemilik data dan tidak

menggunakan sistem keamanan kriptografi oleh karena itu keaslian sistem informasi masih rentan terhadap penyadapan. Dalam penelitian lain mengenai manajemen akases adalah control akses pada aplikasi layanan pemerintah menggunakan model *Design Science Research Methodology* (*DSRM)* dimana proses ini merumuskan persyaratan otentifikasi, otorisasi dan audit berdasarkan kriteria pengguna [3].

Otorisasi user merupakan kuasa atau wewenang yang diberikan kepada user dalam menggunakan atau mengelola sistem informasi web, namun bagaimana jika ada seorang user yang mengakses sebuah halaman padahal halaman tersebut bukan merupakan hak yang diberikan kepada user tersebut, tentunya ini merupakan sebuah kesalahan dalam otororisasi user, maka dari itu dibutuhkan keamanan dalam pemberian hak izin user dalam mengakses database server. Upaya untuk mengatasi permasalahan dalam manajemen akses tersebut dapat digunakan teknik kriptografi dengan mengkombinasikan algoritma RSA (*Rivest Shamir Adleman*) dan algortima AES (*Advanced Encryption Standard*). Kelebihan algoritma RSA adalah terletak pada kehandalannya karena prosesnya yang sangat rumit namun kurang baik terhadap data bersekala besar [4]. Sedangkan algoritma AES sangat cocok pada data yang bersekala besar dengan waktu proses yang cukup cepat namun pendistribusian kunci yang cukup sulit sehingga kehandalan algoritma tergantung pada pemegang kunci tersebut seperti yang dijelaskan pada penelitian sebelumnya [5].

Perbandingan mengenai kinerja dari algoritma RSA dan AES yaitu algoritma AES lebih unggul dibandingkan dengan algoritma RSA, dengan rata-rata proses enkripsi 236 kali lebih cepat dan 2.6 kali lebih cepat dalam proses dekripsi[6]. Dalam penelitian lain mengenai kinerja dari algoritma RSA adalah

proses enkripsi dan dekripsi bergantung pada besarnya pasangan kunci dimana jika pasangan kunci lebih besar maka proses enkripsi dan dekripsi lebih lama. Sedangkan algoritma AES dipengaruhi oleh panjangnya kunci dimana jika semakin panjang kunci yang digunakan maka semakin lama proses enkripsi dan dekripsi[7]. Sedangkan dalam penelitian lain kinerja algoritma RSA bergantung pada nilai pemaktoran diman semakin besar nilai pemaktornya maka semakin lama proses pemecahannya[4].

Advokathan adalah suatu sistem informasi yang menyediakan layanan konsultasi hukum, manajemen dan persidangan dengan tujuan untuk memberikan layanan hukum berkualitas tertinggi dalam bidang hukum Islam dengan jaminan hasil terbaik. Semua data yang ada didalam sistem informasi advokathan adalah data yang brersifat pribadi maka harus memiliki sistem pengamanan yang handal dengan mengkombinasikan algoritma RSA dan AES pada sistem pemberian kewenangan dalam sistem informasi advokathan.

1.2. Perumusan Masalah

Berdasarkan latar belakang diatas dapat diambil beberapa permasalahan yaitu sebagai berikut:

1. Bagaimana menerapkan algoritma *Rivest Shamir Adleman (RSA)* dan algortima *Advanced Encryption Standard (AES)* dalam sistem otorisasi user pada *database server* Advokathan?

2. Bagaimana kinerja algoritma RSA (*Rivest Shamir Adleman*) dan algortima AES (*Advanced Encryption Standard*) dalam sistem otorisasi user pada *database server* Advokathan?

1.3. Tujuan Penelitian

Tujuan penelitian tugas akhir ini adalah untuk menerapkan dan mengetahui kinerja dari algoritma RSA (*Rivest Shamir Adleman*) dan algortima AES (*Advanced Encryption Standard*) dalam sistem otorisasi user pada database server Advokathan

1.4. Manfaat Penelitian

Manfaat penelitian tugas akhir ini adalah sebagai berikut:

1 Sistem yang dibangun dapat digunakan untuk pengamanan data client yang melakukan konsultasi hukum

2 Sistem otorisasi user dapat diterapkan pada aplikasi web lain yang membutuhkan pengamanan data

1.5. Batasan Masalah

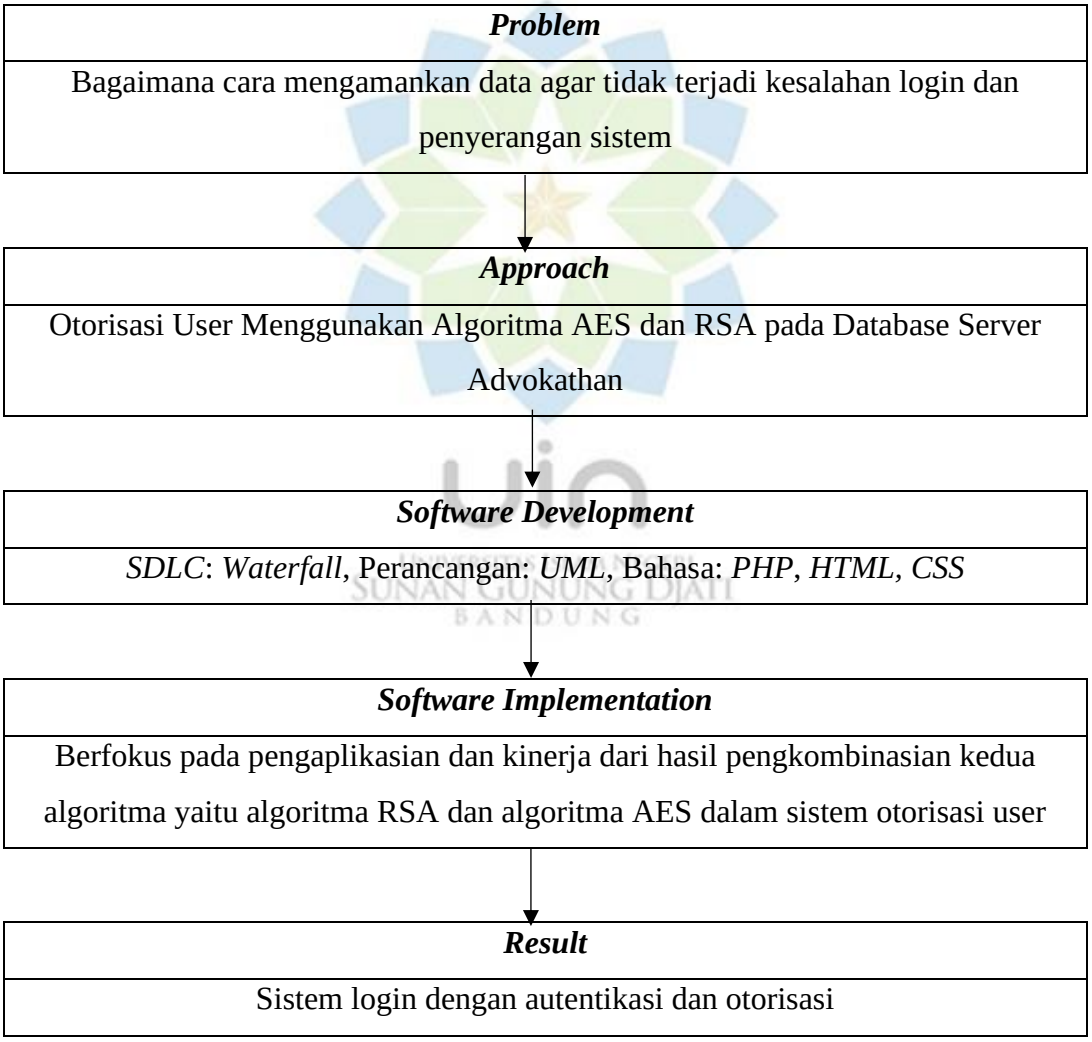
Untuk mempermudah dalam penelitian ini, maka hendaknya membatasi masalah-masalah yang akan dipecahkan yaitu sebagai berikut:

1. Fitur-fitur yang akan dibangun adalah *form r*egister, *login* dan *logout*
2. Algoritma yang digunakan dalam penelitian ini adalah algoritma RSA (*Rivest Shamir Adleman*) dan algortima AES (*Advanced Encryption Standard*)

3. Implementasi dari algoritma RSA (*Rivest Shamir Adleman*) dan algortima AES (*Advanced Encryption Standard*) hanya untuk otorisasi user
4. Advokathan hanya dijadikan sebagai objek penelitian dan tidak membangun sistem informasinya

1.6. Kerangka Pemikiran

Kerangka pemikiran dari Tugas Akhir ini dapat dilihat pada Gambar 1.1 berikut:



Gambar 1. 1 Kerangka Pemikiran

Pada gambar 1.1 diatas dapat diketahui bahwa masalah utama dengan dibuatnya aplikasi ini adalah bagaimana cara mengatasi kesalahan login dan penyerangan dengan menerapkan sistem otorisasi user dengan kombinasi algoritma AES dan RSA pada database server Advokathan. Hasil yang diharapkan adalah data user dapat terjamin keamanannya.

1.7. Metode Penelitian

1.7.1 Teknik Pengumpulan Data

Metode pengumpulan data yang digunakan dalan penilitian ini adalah dengan metode penelitian deskriptif. Metode penelitian ini bertujuan untuk mendeskripsikan gambaran permasalahan dengan lengkap. Berikut adalah teknik yang digunakan dalam pengumpulan data:

a. Wawancara

   Metode ini dilakukan dengan berinteraksi langsung dengan narasumber yang ahli dalam bidang penelitian untuk mendapatkan informasi yang relevan dengan penelitian

b. Observasi

   Metode observasi adalah pengumpulan data dengan cara mengamati secara langsung pada objek penelitian dengan tujuan memperoleh data-data yang dibutuhkan.

c. Studi Literatur

   Metode ini digunakan dengan mempelajari penelitian-penelitian yang telah dilakukan yang ada kaitannya dengan objek penelitian.

1.7.2 Tahap Pengembangan Sistem

Tahapan-tahapan yang digunakan dalam pengembangan sistem adalah dengan model *Waterfall*. Model *waterfall* merupakan suatu metode yang dikenal sebagai model air terjun karena dalam proses membangun sistem, pengembang harus menyelesaikan fase saat ini sebelum melanjutkan fase yang berikutnya [8].

Adapun tahapan-tahapan dalam pengembangan sistem otorisai *use*r dengan menggunakan metode *waterfall* ini dapat dijelaskan sebagai berikut:

1. *Requirements Specification*

   Merupakan tahap awal dalam model waterfall yang bertujuan untuk menganalisa semua kebutuhan yang diperlukan dalam pembangunan proyek tugas akhir ini. Dalam pembangunan sistem otorisasi ini dijelaskan mengenai hardware dan software yang dibutuhkan.

2. *Design*

   Tahap *design* merupakan tahap perancangan desain, pada tahap ini desain sistem otorisasi dirancang mulai dari perancangan desain *user interface* sampai dengan perancangan alur program sistem otorisasi ini.

3. *Implementation*

   Tahap ini adalah proses pengerjaan sistem dengan menerapkan kode program (*Encoding*) berdasarkan hasil perancangan desain yang telah dilakukan pada tahap sebelumnya kedalam bahasa pemrograman. Pada tahap inilah desain

sistem otorisasi yang telah dirancang diimplementasikan sehingga rancangan sebelumnya menjadi suatu model program.

4. *Testing*

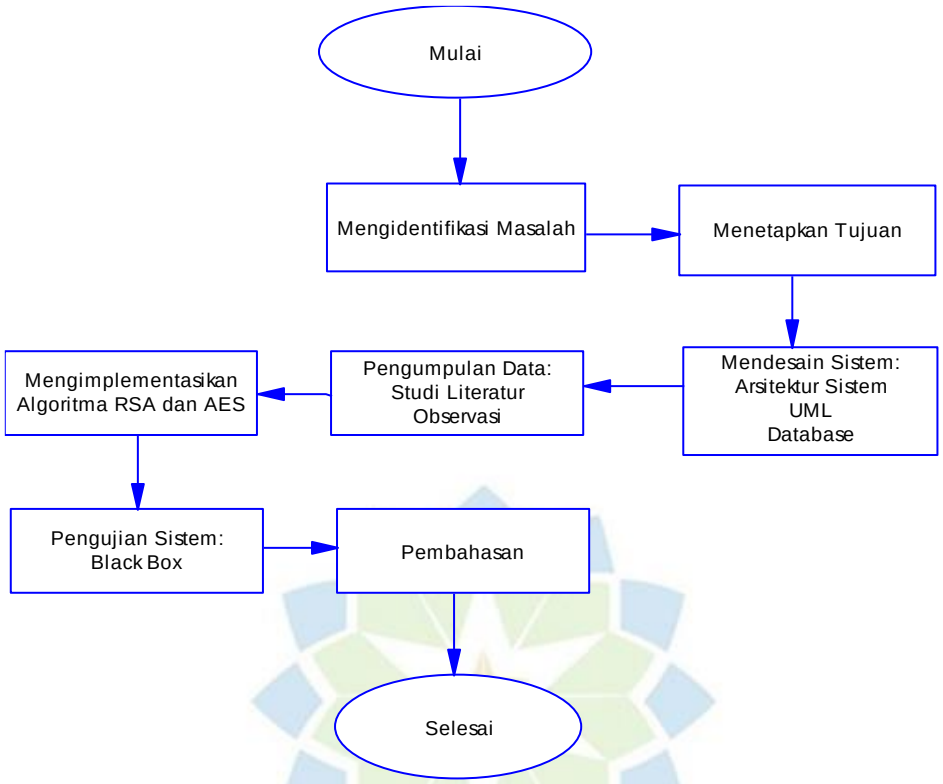
   Tahap ini merupakan pengujian yang dilakukan oleh individu atau kelompok penguji (*Unit Testing*) terhadap seluruh sistem yang telah dibangun

5. *Devloyment and Maintenance*

   Tahapan ini adalah tahap terakhir dari model waterfall yaitu menjalankan sistem yang telah dibangun, memperbaiki bug dan dilakukan pemeliharaan secara berkala

1.7.3 Alur Penelitian

Alur penelitian dari tugas akhir ini dapat dilihat pada gambar 1.2 berikut:



Gambar 1. 2 Alur Penelitian

Berdasarkan gambar 1.2 diatas dapat dijelaskan bahwa alur penelitian ini dimulai dari mengidentifikasi masalah kemudian menetapkan tujuan penelitian. Data-data yang diperlukan dicari melalui studi literatur dan observasi. Setelah data yang diperlukan terkumpul kemudian membuat desain dari arsitektur sistem. Tahap selanjutnya adalah implementasi atau pembuatan sistem dari desain yang telah dibuat. Jika tahap implementasi sistem telah dibuat maka dilakukan pengujian menggunakan metode *blackbox testing*, tujuan mencari kesalahan dari *user interface* fungsi sistem. Selanjutnya tahap terakhir dalam penelitian ini adalah menjelaskan hasil dan pembahasan dari sistem yang telah selesai diuji

1.8. Sistematika Penulisan

Laporan penelitian tugas akhir ini ditulis menggunakan sistematika penulisan agar mudah dipahami. Berikut adalah sistematika penulisan dari tugas akhir ini:

BAB I PENDAHULUAN

Bab 1 merupakan pengantar dan penggambaran masalah-masalah yang akan dibahas. Beberapa pokok bahasan dari bab 1 ini adalah latar belakang, perumusan masalah, manfaat penelitian, Batasan masalah, kerangka pemikiran, metode penelitian, alur penelitian dan sistematika penulisan.

BAB II STUDI PUSTAKA

Bab II merupakan pembahasan teori yang digunakan untuk mecari solusi permasalahan yang telah dibahas pada bab sebelumnya. Pokok bahasan dari bab II ini adalah studi literatur dan kajian teori.

BAB III ANALISIS DAN PERANCANGAN

Pada bab III ini dilakukan analisis dan perancangan terhadap sistem yang akan dibangun. Pokok bahasan dari bab ini adalah analisis kebutuhan sistem, analisis algoritma dan perancangan desain sistem.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab IV ini dijelaskan mengenai kebutuhan, implementasi dan pengujian sistem yang dibangun. Tahap pengujian berfungsi untuk mengetahui fungsionalitas

sistem yang telah dibangun, apakah sudah sesuai dengan kebutuhan dan perancangan atau belum.

BAB V PENUTUP

Bab V adalah kesimpulan yang diambil dari sistem yang telah dibangun yang bersumber dari perumasan masalah pada bab I. pada bab ini juga dijelaskan mengenai saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Daftar pustaka adalah sember teori yang digunakan dalam penelitian dan diambil dari buku, jurnal, *prociding*, atau dari penelitian sebelumnya yang berkaitan dengan pembahasan penelitian.

LAMPIRAN

Lampiran adalah dokumen yang dilampirkan dalam bentuk file, gambar, *source code* dan lain-lain