BAB I
PENDAHULUAN

1.1. Latar Belakang

Masalah keamanan merupakan salah satu aspek penting dari sebuah system informasi, akan tetapi masalah keamanan kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting[1] . Untuk meningkatkan keamanan pada data, maka diperlukan sebuah gembok untuk mengunci data tersebut. Dan yang dapat membuka data tersebut hanyalah pihak yang mempunyai otoritas.

Beberapa hal penting yang harus diperhatikan pada keamanan suatu aplikasi berbasis *web* dan menjadi masalah yang penuh kerentanan adalah *login* dan *database.* Sistem *login* yang menggunakan *database*, sebagai autentikasi *user* dan *password* sangat rentan untuk diretas. SQL *Injection* adalah salah satu teknik serangan yang dapat digunakan oleh penyerang untuk mengeksploitasi aplikasi *web,* sebagai akibatnya penyerang bisa mendapatkan akses tidak sah ke *database* atau untuk mengambil informasi langsung dari *database* [1].

Kriptografi merupakan pilihan yang tepat dalam pengamanan data semacam ini. Algorittma kriptografi dibagi menjadi dua yaitu, algoritma simetris dan asimetris. Kriptografi simetris hanya memakai satu kunci dalam proses enkripsi dan deskripsi.

Seperti yang telah dilakukan peneliti sebelumnya, yaitu tentang Implementasi Algoritma Hill Cipher dalam Penyandian Data, dimana pada penelitian tersebut membahas mengenai proses enkripsi dan deskripsi dengan

teknik *hill cipher* bisa dilakukan pada *record*. Dimana *record* yang ingin diproses dapat ditentukan oleh pemakai untuk pengamanan data pada *record* yang dipilih oleh user. Namun pada penelitian ini masih terdapat kekurangan, diantaranya mengenai pengaplikasiannya yang masih di desktop, dan algoritma yang digunakan lemah jika penyerang sudah mengetahui terlebih dahulu beberapa ukuran dari *matrix key* (*knowplaintext attack*) [2].

Untuk menjawab kekurangan tersebut, pada penelitian ini dilakukan pengembangan enkripsi *key* dengan menggunakan algoritma AES (*Advanced Encryption Standard*) 256 bit. Keunggulan AES dibandingkan dengan algoritma *hill cipher* dan algoritma kriptografi lainnya adalah AES memiliki jumlah bit untuk sub kunci yang lebih banyak dan beragam karena terdapat 3 *block chiper* yang dapat dipakai, lebih efisien pada saat enkripsi sehingga tidak memerlukan waktu yang lama, dan menghasilkan chiper yang lebih besar karena terdapat penambahan header pada saat enkripsi. AES pun efisien untuk diimplementasikan pada perangkat web ataupun android karena penggunaan memori yang sedikit. Selain itu AES pernah dijadikan standar penyandian simetris oleh lembaga standar Amerika Serikat NIST (*National Institute of Standards and Technology*) pada tahun 2001.

Berdasarkan uraian diatas, sehingga penelitian ini fokus terhadap keamanan data dengan judul "Implementasi Algoritma *Advanced Encryption Standar* (AES) sebagai Authentifikasi Key Untuk User pada Aplikasi Chatting Berbasis Web".

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut maka dapat dirumuskan menjadi beberapa masalah diantaranya:

a. Bagaimana menerapkan Algoritma AES (*Algoritma Advanced Encryption Standar*) 256 bit sebagai authetifikasi key untuk user pada aplikasi chatting.
b. Bagaimana kinerja algoritma AES (*Algoritma Advanced Encryption Standar*) 256 bit sebagai authentifikasi key untuk user pada aplikasi chatting.

1.3. Tujuan Penelitian

Berdasarkan permasalahan yang diteliti, tujuan penelitian ini ialah :

a. Menerapkan Algoritma *Advanced Encryption Standar* (AES) 256 bit sebagai Authetifikasi Key Untuk User pada aplikasi chatting sehingga keamanan password dapat terjaga.
b. Mengetahui kinerja dari algoritma *Advanced Encryption Standar* (AES) 256 bit sebagai authentifikasi key untuk user pada aplikasi chatting.

1.4. Batasan Masalah

Batasan masalah dalam membangun aplikasi :

a. Aplikasi ini merupakan perangkat lunak yang berbasis *website.*
b. Metode yang digunakan dalam pembuatan aplikasi ini menggunakan algoritma AES 256 bit.
c. Metode pengembangan perangkat lunak aplikasi ini menggunakan metode *Agile* yaitu *Rational Unifed Process* (RUP).
d. *Feature* yang tersedia adalah authentifikasi untuk user serta proses enkripsi dan dekripsi password pada *database* sistem.
e. Jaringan yang di gunakan pada aplikasi ini adalah jaringan bersifat *public.*
f. Aplikasi yang dibuat merupakan pengembangan hasil karya sendiri

g. Pengembangan aplikasi ini hanya fokus pada proses keamanan dan autentikasi pada saat *register* serta *login.*

h. Metode *Hash* MD 5 digunakan sebagai tambahan enkripsi pada saat sebelum enkripsi AES 256 bit.

1.5. Manfaat Penelitian

Manfaat dari penelitian tugas akhir ini adalah untuk menjaga kerahasiaan data dari kasus pencurian data yang sering terjadi oleh pihak yang tidak bertanggung jawab melalui keamanan sistem dengan cara enkripsi dan dekripsi password dan mengetahui penerapan algoritma *Advanced Encryption Standard* (AES) 256 bit.

1.6. Kerangka Pemikiran

Adapun kerangka pemikiran dari implementasi algoritma AES ini digambarkan pada gambar 1.1 :

1.7. Metode Penelitian

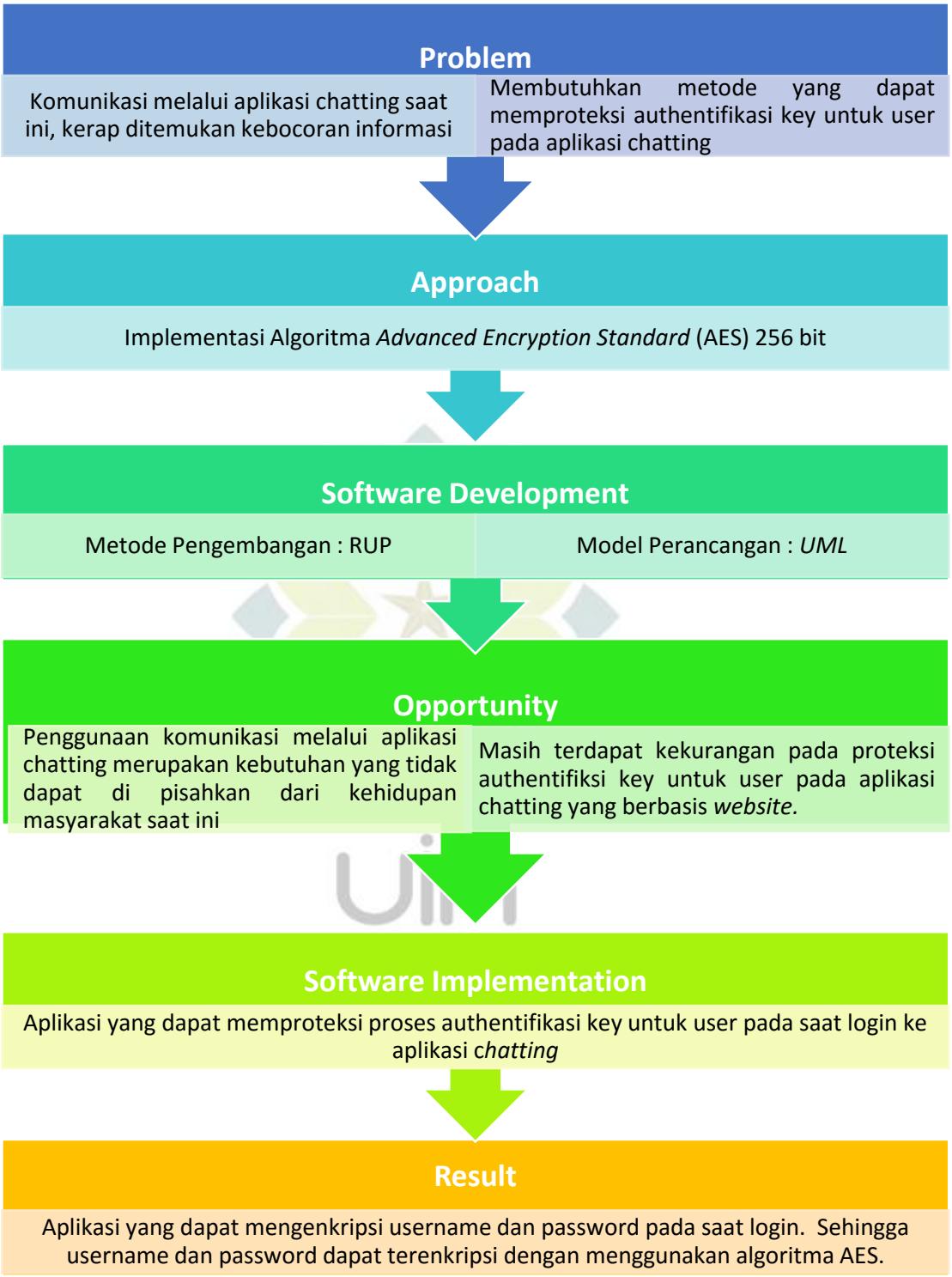
1.7.1. Teknik Pengumpulan Data

1. Observasi

   Teknik pengumpulan data dengan mengadakan penelitian dan peninjauan langsung terhadap permasalahan yang diambil. Hal ini dilakukan pada aplikasi yang telah dibuat sebagai referensi sesuai dengan judul yang diambil.

2. Studi Literatur

   Pengumpulan data dengan cara mengumpulkan literatur, jurnal, *paper* dan bacaan-bacaan yang ada kaitannya dalam pembuatan tugas akhir ini.



Gambar 1.1 Kerangka Pemikiran

1.7.2. Metode Pengembangan Perangkat Lunak

Adapun metode pengembangan perangkat lunak yang akan dibuat yaitu menggunakan metodologi *Agile* yaitu *Rational Unifed Process* (RUP). *Rational Unified Process*, adalah suatu kerangka kerja proses pengembangan perangkat lunak iteratif yang dibuat oleh Rational Software, suatu divisi dari IBM sejak tahun 2003. Dengan menggunakan model ini, RUP membagi tahapan pengembangan perangkat lunaknya ke dalam 4 fase sebagai berikut :

1. *Inception*, merupakan tahap untuk mengidentifikasi sistem yang akan dikembangkan. Proses ini dilakukan pada saat menganalisis penelitian-penelitian yang sudah dilakukan melalui *literature* jurnal nasional dan internasional sebagai acuan yang bersangkutan dengan judul dan merumuskan masalah.
2. *Elaboration*, merupakan tahap untuk melakukan desain secara lengkap berdasarkan hasil analisis di tahap *inception*. Proses ini dilakukan dengan merancang pemodelan aplikasi menggunakan UML, membuat mockup dan dokumentasi.
3. *Construction*, merupakan tahap untuk mengimplementasikan hasil desain dan melakukan pengujian hasil implementasi. Pada tahap ini telah dilakukan pengerjaan *source code (coding)* untuk pembuatan produk aplikasi sesuai dengan analisis dan desain yang telah dilakukan sebelumnya.
4. *Transition*, merupakan tahap untuk menyerahkan sistem aplikasi ke konsumen (*roll-out*), yang umumnya mencakup pelaksanaan pelatihan kepada pengguna dan testing beta aplikasi terhadap ekspetasi pengguna. Pada

tahap ini dilakukan pengujian aplikasi apakah sesuai dengan masalah judul yang diajukan pada tugas akhir dan dituangkan pada kesimpulan.

1.8. Sistematika Penulisan

Sistematika pembuatan perangkat lunak ini dibagi menjadi 5 (lima) bab yang masing-masing bab telah dirancang dengan suatu tujuan tertentu. Berikut penjelasan tentang masing-masing bab.

BAB I PENDAHULUAN

Berisi pembahasan masalah umum yang berhubungan dengan penyusunan laporan tugas akhir yang meliputi latar belakang, rumusan masalah, tujuan, batasan masalah, manfaat penelitian, *state of the art*, kerangka pemikiran, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab II dijelaskan mengenai teori-teori yang berhubungan dengan masalah yang dikemukakan pada penelitin ini, dan juga teori-teori yang digunakan dalam perancangan dan implementasi.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Dalam bab III dibahas mengenai analisis sistem yang mencakup analisis kebutuhan fungsional dan non fungsional, Perancangan sistem, arsitektur algoritma dan perhitungan manual dari algoritma yang digunakan.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Dalam bab IV menguraikan implementasi aplikasi yang telah dianalisa dan dirancang, kemudian dilakukan proses pengujian terhadap aplikasi yang dibangun.

BAB V PENUTUP

Bab V berisi kesimpulan dan saran untuk pengembangan aplikasi lebih lanjut dalam upaya memperbaiki kelemahan pada aplikasi guna untuk mendapatkan hasil kinerja aplikasi yang lebih baik dan pengembangan program selanjutnya.

DAFTAR PUSTAKA

Daftar Pustaka berisi semua sumber tertulis atau tercetak yang pernah dikutip dan digunakan dalam proses penyusunan.

LAMPIRAN

Berisi semua dokumen yang digunakan dalam proses penyusunan dan perancangan seperti *source code*, kelengkapan dokumen dan lain sebagainya