BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi sekarang ini semakin berkembang dan maju, pengguna serta pengembang di tutuntu untuk selalu mengikuti trend yang sedang berkembang agar tidak tertinggal oleh terknologi terbarukan. Komputer yang dahulu berada di meja sekarang beralih di genggaman tangan, tingkat mobilitas yang sangat tinggi memaksa pengembang teknologi untuk membuat sebuah perangkat yang dapat menunjang hal itu, yaitu *smartphone*.

Smartphone, sebuah teknologi yang memadukan fitur telepon standar dengan komputerisasi yang lebih yang memiliki fungsi multitasking. Dahulu pekerjaan dikerjakan dengan komputer, namun sekarang semua itu dapat dikerjakan hanya dengan sebuah *smartphone*. *Browsing*, mengetik dokument, presentsi dan lain sebagainya dapat dengan mudah di kerjakan dengan perangkat tersebut. Berbagi file antar perangkat samartphone juga dapat dilakukan secara langsung menggunakan *bluethooth*, jaringan data dan sebagainya. Namun bagaimana dengan keamanan file yang yang akan di bagikan antar perangkat *mobile*?

Sama halnya dengan komputer *desktop*, berbagi file dengan *smartphone* juga rentan dengan serangan dari pihak luar. Seperti dapat di baca oleh orang yang

bukan penerimanya dan hal lain sebaginya. Bagiaman dengan file yang benar-benar sangat rahasia, namun ingin di kirimkan dengan aman kepada pihak peneima tanpa dikatehu orang yang bukan seharusnya menerima.

Berbagi file antar *smartphone* sekarang ini masih sebatas pengiriman dan penerimaan file saja, tanpa adanya keamanan yang memumpuni sehingga data yang terkirim tidak akan terjaga kerahasiaannya. Aplikasi *mobile* yang dapat berbagi file dan dapat menjaga kerahasiaan file tersebut sangatlah di butuhkan sekarang ini dikarenakan semakin intensnya penggunaan perangkat *smartphone* daripada komputer *desktop*.

Berbagi file antar perangkat smartphone secara umum dilakukan menggunakan media *transfer bluethooth* yang mudah, dengan media *bluethooth* antar perangkat tinggal mengaktifkan *bluethooth* masing-masing. Namun hal ini dapat disusupi oleh pihak yang tidak berhak atas akses tersebut dan masuk dalam area konektifitas *bluethooth* untuk menyadap file hasil transfer antar perangkat tersebut.

Serta ada banyak varian yang dapat dijadikan media berbagi file antar perangkat smartphone yaitu aplikasi perpesanan (*messenger*) seperti *Whatsapp*, *Facebook Messanger* dan lain sebaginya. Di aplikasi tersebut ketika berbagi file sangatlah mudah dan cepat, namun keamanan akan file yang dikirim tersebut tidaklah terjaga kerahasiannya karena penerima pesan file belum tentu orang yang dikehendaki. Dan penerima yang bukan di kehendakitersebut membuka file yang dikirim tersebut secara tidak sengaja di dalam aplikasi tersebut.

Dengan demikian aplikasi *mobile* dengan fungsi pengamanana file sangatlah dibutuhkan untuk menunjang mobilitas pengguna *smartphone*, untuk itu akan di rancang sebuah aplikasi *mobile* yang akan memberikan keamanan pada file yang akan di dibagikan kepada pihak lain antar pengguna *smartphone* agar dapat menjaga kerahasiaan file tersebut.

1.2 Rumusan Malasah

Perumusan masalah dalam skripsi ini adalah sebagai berikut:

a. Bagaiman menerapkan algoritma AES, RSA dan RC6 dalam melindungi data, saat berbagi file ?
b. Bagaimana membangun program aplikasi mobile keamanan berbagi file menggunakan kombinasi algoritma AES, RSA dan RC6, dalam implementasinya terhadap pengamanan berbagi file ?

1.3 Batasan Masalah

Pada skripsi ini penulis membatsi maslah dengan membuat sebuah aplikasi *mobile* yang akan digunakan untuk pengamanan file dan hanya meliputi:

1. Algoritma kriptografi yang digunakan dalam pengamanan file ada tiga yaitu : AES, RSA dan RC6.
2. Berbagi file dilakukan dengan jaringan client server.
3. Aplikasi dijalankan pada sistem operasi Android versi 4.0 *Ice Cream Sandwich* hingga versi 5.0 *Lolipop*.
4. Jenis file yang dapat dienkripsi/dekripsi adalah file dokumen.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Berdasarkan uraian latar belakang dan rumusan masalah diatas, maka maksud dari penelitian ini ialah untuk mangamkankan proses berbagi file (*file sharing*) antar pengguna *smartphone*.

1.4.2 Tujuan Penelitian

Tujuan penelitian yang hendak dicapai ialah membuat Aplikasi Mobile Keamanan Berbagi File Menggunakan Kombinasi Algoritma AES, RSA dan RC6 yang diharapkan mampu membantu melindungi file yang hendak dibagikan dalam penggunaan smartphone, agar menjadi lebih aman dari seseorang yang bukan haknya untuk mengakses *file document* yang bersifat privasi tersebut. Selain itu juga bertujuan untuk merancang sebuah pengamanan terhadap file agar lebih tahan terhadap serangan Brute forece attack.

1.5 Metode Penelitian

1.5.1 Teknik Pengumpulan Data

Adapun teknik pengumpulan data yang digunakan dalam penyusuannan skripsi ini adalah sebagi berikut:

1. Metode Observasi yaitu mengamati objek yang dijadikan sumber penelitian sehingga dapat memperoleh data yang akurat yang kemudian di catat sebagi bahan analisa.

2. Metode Kepustakaan

   Yaitu metode pengumpulan data yang dilakukan dengan cara membaca dan mempelajari buku-buku sebagai refrensi sehingga data dapat diperoleh dari literature majalah, publikasi dan bio statistic. Serta sumber-sumber yang berkaitan dengan permasalahan dalam penelitian.

1.5.2 Metode Analisis

Analisis terhadap hal-hal yang dibutuhkan dalam pengembangan perangkat lunak yang terdiri dari:

a. Analisi deskripsi object data menggunakan UML (*Unified Modelling Language*).
b. Analisis spesifikasi proses melalui UCD (*Use case Diagram*).

1.5.3 Metode Perancangan

Perancangan adalah suatu tahapan penggambaran terhadap data-data yang telah dikumpulkan sehingga dapat digunakan untuk pengembangan perangkat lunak. Tahap perancangan secara umum bisa dibagi sebagai berikut:

1. *Logical Design* merupakan perancangan yang dapat dilakukan tanpa tergantung dengan *platform* atau teknologi yang akan digunakan untuk mengimplementasikan sistem. Jenis perancangan semacam ini biasa dilakukan sebelum menentukan teknologi yang akan digunakan dalam sistem.
2. *Physical Design* merupakan perancangan yang lebih detil daripada *logical design*, dan hasilnya spesifik kepada platform tertentu, karena

perancangan ini memperhatikan/tergantung kepada jenis teknologi yang akan digunakan untuk mengimplementasikan sistem.

1.5.4 Metode Pengembangan

Pada tahap ini dilakukan proses pengembangan untuk menyusun suatu sistem yang baru menggantikan sistem yang lama secara keseluruhan/memperbaiki sistem yang telah ada. Dimana metode pengembangan sistem *waterfall*.

1.5.5 Metode Pengujian Unit

Pada tahap ini dilakukan proses pengujian dalam lingkungan yang telah didefinisikan sebelumnya.

1.5.6 Metode Implementasi

Pada tahap ini dilakukan proses penerapan data yang terkumpul kedalam bahasa pemrogaman komputer. Dalam pengkodean pada masalah ini menggunakan bahasa pemrograman Java dengan *tool* IDE Android Studio / Eclipse dan berbasis Java lainnya.

1.6 Sistematika Penulisan

Untuk lebih memahami pembahasan yang terdapat pada proposal skripsi ini, maka penulisan materi yang akan disampaikan disusun dalam sistematika ebagai berikut:

1. BAB I PENDAHULUAN

   Pada bab ini akan dibahas latar belakang maalah, rumusan masalah, batasan masala, tujuan penelitian, manfaat penelitian , metode penelitian dan sistematika penulisan.

2. BAB II LANDASAN TEORI

   Bab ini akan menjelasakn tentang landasan teori yang digunakan dalam proses perancangan dan pembuatan sebauh aplikasi *mobile* dan teori-teori yang berhubungan dengan kriptografi.

3. BAB III ANALISI DAN PERANCANGAN SISTEM

   Bab ini berisi tentang uraian analisi dan perancangan aplikasi, analisi studi kelayakan sistem, desain *interface*, *activity* diagram dan juga analisis sesuai dengan tema yang digunakan pada Aplikasi *Mobile* Kemanan Berbagi File Menggunakan Kombinasi Algoritma AES, RSA dan RC6.

4. BAB IV IMPLEMANTASI DAN PEMBAHASAN

   Bab ini berisi tentang implemantasi , bagaimana cara menjalankan aplikasi, kelebihan dan kekuarang aplikasi, serta evaluasi tehadap hasil yang telah dicapai dari aplikasi yang telah dikembangkan.

5. BAB V PENUTUP

   Bab ini berisi mengenaik kesimpulan dan saran yang berkaitan dengan skripsi yang telah dibuat untuk pengembangan lebih lanjut dikemudian hari.

6. DAFTAR PUSTAKA

Dalam bab ini berisi tentang pustaka yang digunakan penulis sebagai acuan dan bahan dalam pembuatan skripsi.