BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan telepon seluler baik dari segi teknologi maupun modelnya memang sangat pesat, teknologi perangkat lunak telah menambahkan fungsi sebuah ponsel bukan hanya sekedar telepon dan *SMS*, kini ada juga *mobile application* yang merupakan aplikasi yang dapat berjalan di ponsel dan dapat dijadikan sebagai bentuk dari media informasi, media belajar ataupun sebagai media hiburan.

Seiring dengan tingkat mobilitas yang sangat tinggi, beberapa tahun terakhir tengah marak perangkat bergerak. Salah satu perangkat *mobile* yang paling pesat dan berkembang adalah *smartphone* berbasis android, di mana hampir setiap orang memilikinya. Hingga saat ini Android terus berkembang baik secara sistem maupun aplikasinya. Salah satu aplikasi yang saat ini berkembang adalah aplikasi *File Sharing*.

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

File sharing adalah aktifitas dimana para pengguna internet dapat berbagi *file* dengan pengguna internet lainnya dengan cara penyedia *file* terlebih dahulu meng-*upload file* ke komputer server dan kemudian para pengguna internet yang lainnya dapat mendownload *file* tersebut dari komputer server.

Seiring dengan tingkat keamanan pada *file* yang semakin rentan terhadap peretasan, kemungkinan peretasan dapat terjadi pada saat *sharing* atau pertukaran informasi, maka dibutuhkan sebuah algoritma yang dapat memproteksi *file* adalah algoritma *Advanced Standard Encryption* (AES). AES adalah algoritma simetris

yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu: AES 128-bit, AES 192-bit, dan AES 256-bit. Dari ketiga tipe tersebut selain memiliki tingkat keamanan yang tinggi, proses waktu enkripsi dan dekripsi AES 128-bit lebih cepat dibandingkan dengan tipe kunci yang lain.[1]

Atas dasar tersebut di atas, maka dalam tugas akhir ini mengambil judul "**Implementasi Algoritma *Advanced Encryption Standard* (AES) 128-bit Pada Aplikasi Sharing Dokumen Berbasis Android**"**.**

1.2 Rumusan Masalah

Beradasarkan pada latar belakang di atas, maka masalah yang dapat dirumuskan dalam proses pembangunan sistem ini adalah:

1. Bagaimana membuat *Aplikasi Sharing Dokumen* berbasis Android.
2. Bagaimana menerapkan Algoritma *Advanced Encryption Standard (AES) 128-bit* pada Aplikasi *Sharing* Dokumen*?*
3. Bagaimana kinerja Algoritma *Advanced Encryption Standard (AES) 128-bit?*

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

1.3 Tujuan Penelitian

Tujuan yang hendak dicapai dalam proses pembuatan aplikasi ini adalah :

1. Membuat *Aplikasi Sharing Dokumen* berbasis Android.
2. Menerapkan Algoritma *Advanced Encryption Standar (AES) 128-bit* pada *Aplikasi Sharing Dokumen.*
3. Mengetahui kinerja Algoritma *Advanced Encryption Standar (AES) 128-bit* untuk keamanan data.

1.4 Batasan Masalah

Dalam proses pengerjaan aplikasi yang dirancang akan dibatasi. Adapun batasan masalah yang melingkupi kinerja sistem ini yaitu:

1. *Aplikasi Sharing Dokumen* hanya akan berjalan pada smartphone bersistem operasi Android.
2. Proses enkripsi dan dekripsi hanya digunakan untuk data .doc, .ppt, .xls, .txt, dan .pdf.
3. Proses enkripsi dan dekripsi yang digunakan yaitu dengan metode AES (*Advanced Encryption Standard*) *128-bit*.
4. Batas maksimal dokumen 20Mb.
5. Aplikasi ini dirancang menggunakan bahasa pemograman *Java.*
6. Menggunakan *Firebase Realtime Database* untuk penyimpanan data dokumen.
7. Fitur yang terdapat dalam aplikasi ini adalah:
   a. Sistem *login* yang menggunakan akun Google.
   b. Pengguna dapat merubah/mengedit dokumen.
   c. Pengguna dapat menambahkan pertemanan

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

1.5 Metodologi Penelitian

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data merupakan teknik atau cara yang dilakukan untuk mengumpulkan data. Metode penelitian yang akan digunakan ada Studi Literatur. Studi literatur adalah metode pengumpulan data yang tidak ditujukan

langsung kepada subjek penelitian. Studi dokumen adalah jenis pengumpulan data yang meneliti berbagai macam dokumen yang berguna untuk bahan analisis.

1.5.2 Metode Pengembangan Perangkat Lunak

Metode yang digunakan untuk pengembangan aplikasi ini yaitu metode *Prototype*. *Prototype* merupakan teknik analisis data dalam pengembangan perangkat lunak menggunakan model prototipe. Pendekatan prototipe atau *prototyping* paradigma sangat cocok digunakan untuk sistem atau perangkat lunak yang dibangun mengikuti kebutuhan pengguna, metode ini sangat sesuai diterapkan dalam proses perancangan perangkat lunak yang akan dibangun yang menitik-beratkan pada pendekatan aspek desain, fungsi, dan *user-interface*.[11]

Dengan model prototipe ini perancang dan pengguna bertemu untuk mendefinisikan secara obyektif keseluruhan perangkat lunak, mengidentifikasikan kebutuhan yang diketahui, dan area lebih besar dimana definisi lebih jauh merupakan keharusan kemudian dilakukan perancangan kilat berupa maket atau prototipe sistem untuk kemudian dievaluasi pengguna untuk menyaring kebutuhan pengembangan perangkat lunak.

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

Tahapan-tahapan dalam metode *Prototype* adalah sebagai berikut:

a. Pengumpulan kebutuhan

   Pengguna dan pengembang bersama-sama mendefinisikan format seluruh perangkat lunak, mengidentifikasikan semua kebutuhan, dan garis besar sistem yang akan dibuat.

b. Membangun *prototyping*

   Membangun *prototyping* dengan membuat perancangan sementara yang berfokus pada penyajian kepada pengguna. Perancangan sementara berupa

rancangan perangkat lunak dengan menggunakan *Unifed Modelling Language (UML)*.

c. Evaluasi *prototyping*

Evaluasi ini dilakukan oleh pelanggan apakah *prototyping* yang sudah dibangun sudah sesuai dengan keinginan pengguna. Jika sudah sesuai maka langkah (d) akan diambil. Jika tidak *prototyping* direvisi dengan mengulangi langkah (a), (b), dan (c).

d. Mengkodekan sistem

Dalam tahap ini, *prototyping* yang sudah di sepakati diterjemahkan ke dalam bahasa pemrograman java.

e. Menguji sistem

Setelah sistem sudah menjadi suatu perangkat lunak yang siap pakai, harus dites dahulu sebelum digunakan. Pengujian ini dilakukan dengan *White Box* dan *Black Box Testing*.

f. Evaluasi sistem

Pelanggan mengevaluasi apakah sistem yang sudah jadi sesuai dengan yang diharapkan. Jika ya, maka lanjut ke langkah berikutnya atau poin (g), jika tidak maka ulangi langkah (c) dan (e).

g. Menggunakan sistem

Perangkat lunak yang telah diuji dan diterima pelanggan siap untuk digunakan.

Berikut beberapa keuntungan menggunakan model *prototype* pada pengembangan perangkat lunak yaitu adanya komunikasi yang baik antara pengembang dan pengguna, pengembang dapat bekerja lebih baik dalam menentukan kebutuhan pengguna, pengguna berperan aktif dalam pengembangan sistem, lebih menghemat waktu

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

dalam pengembangan sistem, dan penerapan menjadi lebih mudah karena pengguna mengetahui apa yang diharapkannya.

1.6 Sistematika Penulisan

Sistematika penulisan proposal judul ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan proposal judul ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab I menguraikan latar belakang, perumusan masalah yang merumuskan berbagai masalah yang diteliti secara lebih jelas, tujuan penelitian yang berisi tentang tujuan dilakukannya penelitian, manfaat penelitian, batasan masalah untuk memberikan batasan yang tegas dan jelas serta sistsematika penyusunan yang menguraikan urutan penyajian yang digunakan dalam penyususnan skripsi ini.

BAB II LANDASAN TEORI

Bab II membahas tentang landasan teori dari topik penulisan skripsi secara mendalam beserta referensinya.

BAB III ANALISIS DAN PERANCANGAN

Bab III akan menguraikan hasil analisis dan perancangan aplikasi yang akan dibangun.

BAB IV IMPLEMENTASI

Bab IV akan menguraikan implementasi aplikasi yang telah dianalisa dan dirancang sebelumnya.

BAB V PENUTUP

Bab V berisi uraian tentang kesimpulan dan saran terhadap aplikasi yang hendak dibangun dan dikembangkan lebih lanjut.

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

DAFTAR PUSTAKA

Daftar Pustaka berisi semua sumber tertulis (buku, artikel jurnal, dokumen resmi, atau sumber-sumber lain dari internet) atau tercetak (CD, video, filmatau kaset) yang pernah dikutip dan digunakan dalam proses penyusunan.

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG