

BAB I

PENDAHULUAN

1.1 Latar Belakang

Komunikasi data merupakan hal penting pada teknologi saat ini. Komunikasi data berhubungan erat dengan pengiriman data dengan menggunakan sistem transmisi elektronik dari satu terminal komputer ke terminal komputer yang lain (Marselina, 2013). Komunikasi data berlangsung semakin cepat dengan kapasitas yang semakin besar seiring berjalannya waktu. Hal di atas dapat diwujudkan dengan unit proses dan media penyimpanan yang mumpuni.

Di zaman sekarang ini, *smartphone* merupakan perangkat *mobile* yang memiliki teknologi paling maju dan paling banyak digunakan. Menurut GlobalWebIndex (2015), pada awal Januari 2015, 80% pengguna *internet* memiliki *smartphone*. Sementara itu, 54% dari perangkat *mobile* menggunakan sistem operasi Android (GlobalWebIndex, 2015). Dari data di atas dapat diambil kesimpulan bahwa *smartphone* berbasis *Android* paling banyak dipakai sehingga diputuskan untuk menggunakan *smartphone* berbasis *Android* sebagai target implementasi.

Komunikasi data lewat *smartphone* sudah menjadi hal yang biasa pada saat ini. Namun, kemampuan komunikasi data *smartphone* masih kalah dengan komputer saat ini. Hal tersebut salah satunya disebabkan karena media penyimpanan yang terbatas (Pande, 2013). Dibutuhkan metode yang dapat mengecilkan data pada *smartphone* tetapi isi data tetap utuh. Masalah tersebut

dapat dipecahkan dengan mengurangi ukuran data menggunakan teknik kompresi data (Sayood, 2006).

Menurut Sayood (2006), kompresi data adalah suatu teknik mengurangi jumlah bits yang diperlukan untuk merepresentasikan informasi dalam bentuk yang lebih padat. Data yang dikompresi dapat berupa karakter huruf, gambar, suara ataupun urutan dari angka yang didapat dari suatu proses.

Smartphone juga menghadapi keterbatasan pada kemampuan komputasi data dengan cepat (Pande, 2013). Algoritma kompresi LZ4 yang diciptakan oleh Yann Collet (2011) mampu memecahkan permasalahan tersebut. LZ4 menawarkan kecepatan kompresi yang sangat cepat jika dibandingkan dengan algoritma kompresi saat ini.

File di dalam *smartphone* umumnya berupa data pribadi seperti foto, video, dan musik. Bila *file-file* tersebut tidak diberi lapisan keamanan, maka tidak ada yang dapat mencegah orang yang bukan merupakan pemilik *smartphone* untuk mengakses *file-file* tersebut (Dörflinger, 2010). Oleh karena itu, dibutuhkan suatu metode pengamanan yang dapat memberi tambahan keamanan pada *file-file* di dalam *smartphone*.

Algoritma enkripsi AES-256 merupakan standar enkripsi yang diadopsi oleh pemerintah Amerika Serikat (NIST, 2011). Biryukov dan Khovratovich (2009) pada penelitian yang berjudul “*Related Key Cryptanalysis of the Full AES-192 and AES-256*” menggunakan *related-key boomerang attacks* untuk menguji keamanan algoritma AES-256. Hasil pengujian menyatakan bahwa dari sekian

teknik penyerangan yang dicoba tidak ditemukan adanya ancaman yang nyata pada aplikasi yang menggunakan algoritma AES-256.

Berdasarkan latar belakang yang telah dikemukakan di atas, dibutuhkan sebuah aplikasi yang dapat digunakan untuk melakukan kompresi *file* menggunakan algoritma LZ4 dan enkripsi *file* hasil kompresi menggunakan algoritma AES-256 pada *smartphone*.

1.2 Rumusan Masalah

Dari latar belakang tersebut, rumusan masalah dari penelitian dapat dijabarkan sebagai berikut.

1. Bagaimana mengimplementasikan algoritma LZ4 untuk melakukan kompresi *file* pada *smartphone* berbasis Android?
2. Bagaimana mengimplementasikan algoritma AES-256 untuk melakukan enkripsi *file* hasil kompresi menggunakan algoritma LZ4 pada *smartphone* berbasis Android?
3. Bagaimana performa kompresi aplikasi hasil implementasi dibandingkan dengan aplikasi lain yang menggunakan algoritma kompresi sejenis?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut.

1. *Smartphone* yang digunakan pada penelitian adalah *smartphone* dengan sistem operasi Android API Level 21 atau lebih.

2. *File* yang digunakan dalam penelitian adalah *file* dari *Silesia corpus* (Deorowicz, 2003) berjumlah 12 *file* dengan ukuran *file* 6–51 MB.
3. Aplikasi hasil implementasi dibandingkan dengan aplikasi RAR yang menggunakan algoritma berbasis LZSS (Salomon, 2007).
4. Aplikasi hanya dapat melakukan proses kompresi dan enkripsi pada satu *file* dalam satu waktu.
5. Aplikasi hanya dapat melakukan proses dekripsi dan dekompresi pada satu *file* dalam satu waktu.
6. *File* yang dapat digunakan dalam proses dekripsi dan dekompresi adalah *file* hasil keluaran proses kompresi dan enkripsi aplikasi.
7. Aplikasi digerakkan menggunakan layar sentuh pada layar Android.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai dari penelitian ini adalah sebagai berikut.

1. Mengimplementasikan algoritma LZ4 untuk melakukan kompresi *file* pada *smartphone* berbasis Android.
2. Mengimplementasikan algoritma AES-256 untuk mengamankan *file* hasil kompresi menggunakan algoritma LZ4.
3. Mengetahui performa kompresi aplikasi hasil implementasi dibandingkan dengan aplikasi lain yang menggunakan algoritma kompresi sejenis.

1.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah menghemat kapasitas penyimpanan data dan menghemat waktu untuk melakukan kompresi *file* serta memberi keamanan pada *file*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan skripsi ini dijelaskan sebagai berikut.

Bab I Pendahuluan

Berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Berisi landasan teori terkait dengan kompresi data, metode kompresi data, *lossless data compression*, *dictionary based compression algorithm*, algoritma kompresi LZ4, algoritma enkripsi, algoritma enkripsi AES, Android, dan *Silesia corpus*.

Bab III Metodologi Penelitian dan Perancangan Sistem

Berisi metode penelitian dan rancangan aplikasi yang akan dibuat.

Bab IV Implementasi dan Uji Coba

Berisi hasil implementasi dari rancangan yang telah dibuat dan pengujian atas penelitian yang dilakukan serta hasil pengujian.

Bab V Simpulan dan Saran

Berisi kesimpulan penelitian dan saran untuk penelitian selanjutnya.