IMPLEMENTASI ALGORITMA LZ4 DAN AES-256 UNTUK KOMPRESI DAN PENGAMANAN FILE PADA SMARTPHONE BERBASIS ANDROID

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S. Kom.)

Darwin Candra

12110110057

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2016

HALAMAN PENGESAHAN

IMPLEMENTASI ALGORITMA LZ4 DAN AES-256 UNTUK KOMPRESI DAN PENGAMANAN FILE PADA SMARTPHONE BERBASIS ANDROID

Oleh

Nama	: Darwin Candra
NIM	: 12110110057
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi dan Komunikasi

Tangerang, 18 Agustus 2016

Mengetahui,

Ketua Sidang	Dosen Penguji
Dennis Gunawan, S. Kom., M.Sc.	Marcel Bonar Kristanda, S. Kom., M.Sc.

Dosen Pembimbing

Yustinus Widya Wiratama, S.Kom., M.Sc.

Ketua Program Studi

Maria Irmina Prasetiyowati, S.Kom., M

LEMBAR PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya:

Nama	: Darwin Candra
NIM	: 12110110057
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi dan Komunikasi

Skripsi yang berjudul "**Implementasi Algoritma LZ4 dan AES-256 untuk Kompresi dan Pengamanan File pada Smartphone Berbasis Android**" merupakan karya ilmiah pribadi saya, bukan karya ilmiah yang ditulis oleh orang atau lembaga lain, dan semua karya ilmiah orang lain yang dirujuk dalam laporan skripsi ini telah saya sebutkan sumber kutipannya serta dicantumkan dalam Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah skripsi yang saya tempuh.

Tangerang, 18 Agustus 2016

Darwin Candra

IMPLEMENTASI ALGORITMA LZ4 DAN AES-256 UNTUK KOMPRESI DAN PENGAMANAN FILE PADA SMARTPHONE BERBASIS ANDROID

ABSTRAK

Penelitian sebuah Market Research Firm pada tahun 2015 menyatakan bahwa 80% dari pengguna *internet* telah memiliki *smartphone*, di mana 54% dari *smartphone* yang dimiliki menggunakan sistem operasi Android. Proses komunikasi data pun dapat berlangsung dengan mudah antar sesama pengguna *smartphone*. Kendala pada hal ini terletak pada kemampuan komputasi *smartphone* yang masih lambat dan juga pada media penyimpanan yang masih terbatas. Untuk mengatasi hal ini, diperlukan sebuah metode yang tidak hanya mampu melakukan kompresi data, tetapi juga mampu melakukan kompresi dengan cepat. Selain itu, *file-file* di dalam *smartphone* umumnya berupa data pribadi yang bila tidak diberi lapisan keamanan, *file-file* tersebut dapat diakses oleh orang lain tanpa ada pencegahan. Hal di atas dapat diatasi dengan memberi tambahan keamanan pada *file-file* di dalam *smartphone*. Penerapan algoritma LZ4 di dalam aplikasi merupakan bentuk upaya yang dilakukan untuk melakukan kompresi data menjadi bentuk yang lebih padat. Algoritma LZ4 digunakan karena menjanjikan kecepatan kompresi data yang tinggi. Untuk menjaga keamanan dari data yang telah dikompresi, maka diterapkan juga algoritma AES-256 yang merupakan standar enkripsi yang telah diadopsi pemerintah Amerika Serikat sejak tahun 2001. Dari hasil penelitian, terbukti bahwa implementasi algoritma LZ4 memiliki *compression ratio* sebesar 45.02% dan kecepatan kompresi sebesar 9.75 MB/s. Hal ini membuktikan bahwa algoritma LZ4 memiliki kecepatan kompresi yang tinggi, namun dengan *compression ratio* yang rendah. Proses enkripsi menggunakan algoritma AES-256 membutuhkan waktu sekitar 298 ms dengan *throughput* sebesar 27.14 MB/s.

Kata kunci : LZ4, AES-256, Android, Kompresi, Enkripsi

LZ4 AND AES-256 ALGORITHM IMPLEMENTATION FOR COMPRESSING AND SECURING FILE ON ANDROID BASED DEVICE

ABSTRACT

Based on research by a Market Research Firm in 2015 revealed that 80% of internet users personally own smartphone, where 54% of smartphone were using the Android operating system. Data communication can also be done easily among the smartphone users. The problem in this case lies in the smartphone's computing power and its limited media storage. A method was needed to not only able to perform data compression, but also capable of performing the compression quickly. Moreover, the files on smartphone generally consist of personal data which if not given a layer of security, will be easy to be accessed by other people without any prevention. The problem above can be prevented by giving additional security to the files in the smartphone. LZ4 algorithm implementation in the application was an effort made to compress the data into a more compact form. LZ4 was used because it promised high data compression speed. AES-256 which is an encryption standard that has been adopted by US government since 2001 was also implemented to secure the compressed data. The research result showed that LZ4 implementation has compression ratio of 45.02% and compression speed of 9.75 MB/s. It can be concluded that LZ4 compression algorithm provides high compression speed, but with low compression ratio. The encryption process using AES-256 took about 298 ms with the throughput of 27.14 MB/s.

Keywords: LZ4, AES-256, Android, Compression, Encryption

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas berkah dan kuasa yang berlimpah sehingga penulis dapat menyelesaikan laporan kerja skripsi ini. Laporan kerja skripsi yang berjudul "Implementasi Algoritma LZ4 dan AES-256 untuk Kompresi dan Pengamanan File pada Smartphone Berbasis Android" diajukan kepada Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Komunikasi, Universitas Multimedia Nusantara.

Penulis menyadari bahwa tanpa bantuan dari banyak pihak, penulis tidak mungkin dapat menyelesaikan masa skripsi dan juga laporan ini dengan baik. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Ibu Maria Irmina Prasetiyowati, S.Kom., M.T., selaku Ketua Program Studi Teknik Informatika yang telah mendukung penulis dalam pelaksanaan skripsi,
2. Bapak Yustinus Widya Wiratama, S.Kom., M.Sc. selaku Dosen Pembimbing yang telah banyak memberikan masukan dan bantuan dalam proses skripsi dan penulisan laporan,
3. Kedua orang tua penulis yang telah membesarkan penulis sehingga sampai pada jenjang pendidikan ini. Terima kasih atas didikan, motivasi, dan doa yang telah diberikan,
4. Rio Jeffrianto Suwandy, teman baik penulis yang selalu bersedia mendengar keluh kesah penulis, dan
5. Teman-teman angkatan 2012 yang telah menjadi sahabat sekaligus keluarga dalam menuntun ilmu.

Penulis meminta maaf bila terdapat kesalahan dalam pembuatan laporan skripsi ini. Laporan skripsi ini dibuat dengan harapan dapat digunakan oleh pembaca sebagai pedoman untuk mendapatkan informasi yang diinginkan. Akhir kata, penulis berharap laporan skripsi ini dapat digunakan untuk penelitian atau pengembangan aplikasi berikutnya di masa depan.

Tangerang, 18 Agustus 2016

Darwin Candra

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR