ENKRIPSI FILE CITRA MEDIS MENGGUNAKAN AES PADA ANDROID

SKRIPSI

Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
Pada Jurusan Ilmu Komputer / Informatika

Disusun Oleh:
ISA FERRY CHRISWANTORO
J2F007023

JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2014

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Isa Ferry Chriswantoro

NIM : J2F007023

Judul : Enkripsi File Citra Medis Menggunakan AES pada Android

Dengan ini saya menyatakan bahwa dalam tugas akhir/skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 29 Agustus 2014

Isa Ferry Chriswantoro

J2F007023

HALAMAN PENGESAHAN

Judul : Enkripsi File Citra Medis Menggunakan AES pada Android

Nama : Isa Ferry Chriswantoro

NIM : J2F007023

Telah diujikan pada sidang tugas akhir pada tanggal 29 Agustus 2014 dan dinyatakan lulus pada tanggal 29 Agustus 2014

Mengetahui,
Ketua Jurusan Ilmu Komputer / Informatika
FSM UNDIP

Nurdin Bahtiar, S.Si, M.T
NIP 19790720 200312 1 002

Semarang, 29 Agustus 2014
Panitia Penguji Tugas Akhir
Ketua

Aris Sugiharto, S.Si, M.Kom
NIP 19710811 199702 1 004

HALAMAN PENGESAHAN

Judul : Enkripsi File Citra Medis Menggunakan AES pada Android

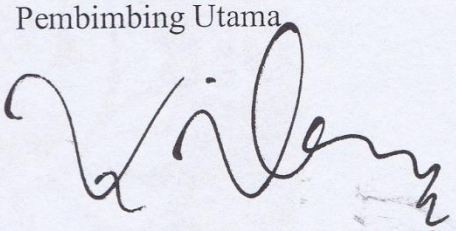
Nama : Isa Ferry Chriswantoro

NIM : J2F007023

Telah diujikan pada sidang tugas akhir pada tanggal 29 Agustus 2014.

Semarang, 29 Agustus 2014

Pembimbing Utama



Helmie Arif Wibawa, S.Si, M.Cs.

NIP 19780516 200312 1 001

ABSTRAK

Citra medis sebagai salah satu data digital dalam bentuk citra yang menyimpan informasi pasien, perlu dilindungi agar informasi pasien terjaga kerahasiaan dan keamanannya. Citra medis yang ada pada media penyimpanan digital biasanya tidak memiliki perlindungan keamanan, sehingga citra medis tersebut dapat dilihat oleh semua orang. Untuk memenuhi aspek kerahasiaan dan keamanan file citra medis, dapat digunakan kriptografi. Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Dengan kriptografi, file citra medis dapat disimpan dengan aman dan rahasia pada media penyimpanan digital. Aplikasi Enkripsi File Citra Medis dibangun untuk mengatasi permasalahan tersebut. Aplikasi ini menggunakan algoritma AES dalam proses enkripsi dan dekripsi file citra medis. AES (*Advanced Encryption Standard*) merupakan algoritma kriptografi yang aman untuk melindungi data atau informasi yang bersifat rahasia. AES merupakan standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya. Aplikasi ini dibangun menggunakan bahasa pemrograman java dan diimplementasikan pada telepon seluler berbasis android. Hasil keluaran dari aplikasi ini berupa file citra medis terenkripsi yang gambarnya tidak bermakna dan dapat pula berupa file citra medis terdekripsi yang dapat dilihat gambarnya jika kunci dekripsi yang dimasukkan benar.

Kata kunci: Citra Medis, AES, Enkripsi, Dekripsi, Android.

ABSTRACT

Medical image as one of the digital data in the form of imagery that stores patient information, must be protected in order to protect the confidentiality and security of patient information. Digital image available on digital storage media usually do not have security protection, so that the digital image can be seen by everyone. To meet the confidentiality and security of medical image files, cryptography can be used. Cryptography is one of the techniques used to enhance the security aspect of the information. With cryptography, medical image files can be stored safely and confidentially on digital storage media. Medical Image File Encryption Application built to overcome these problems. This application uses the AES algorithm in the process of encryption and decryption of medical image files. AES (Advanced Encryption Standard) is a secure cryptographic algorithms to protect data or confidential information. AES is the latest standard cryptographic algorithms published by NIST (National Institute of Standards and Technology) as a replacement for the DES algorithm (Data Encryption Standard), which is over its service life. This application was built using the Java programming language and implemented on a mobile phone based on Android. The output of this application form encrypted medical image files that the picture is not meaningful and can also be decrypted medical image files that can be seen if the decryption key is entered correctly.

Keywords: Medical image, AES, Encryption, Decryption, Android.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul "Enkripsi File Citra Medis Menggunakan AES pada Android"

Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer / Informatika Fakultas Sains Dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan tugas akhir ini, penulis mendapat bantuan dan dukungan dari banyak pihak. Atas peran sertanya dalam membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada:

1. Bapak Dr. Muhammad Nur, DEA selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Bapak Nurdin Bahtiar, S.Si, M.T Ketua Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
3. Bapak Indra Waspada, ST, M.TI selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
4. Bapak Helmie Arif Wibawa, S.Si, M.Cs selaku dosen pembimbing yang selalu memberi arahan agar laporan tugas akhir ini terselesaikan.
5. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu. Semoga Allah membalas segala kebaikan yang telah Anda berikan kepada penulis.

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan tugas akhir ini, untuk itu penulis mohon maaf dan mengharapkan saran serta kritik yang membangun dari pembaca. Semoga laporan tugas akhir ini dapat bermanfaat bagi pengembangan ilmu dan pengetahuan, khususnya pada bidang Informatika.

Semarang, 29 Agustus 2014

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir mengenai Enkripsi File Citra Medis Menggunakan AES pada Android.

1.1. Latar Belakang

Citra medis sebagai salah satu data digital dalam bentuk citra yang menyimpan informasi pasien, perlu dilindungi agar informasi pasien terjaga kerahasiaan dan keamanannya. Misalnya foto *rontgen* dengan sinar-X atau foto penyakit yang terlihat pada tubuh pasien dengan bantuan komputer (Sherrow, 2007). File citra medis dapat dibuka dengan menggunakan aplikasi pembuka gambar yang ada pada sistem operasi, salah satunya adalah android.

Android merupakan sistem operasi berbasis linux yang dirancang untuk perangkat *mobile* seperti telepon pintar dan komputer tablet. Sebagai perangkat *mobile* android memiliki beberapa kelebihan dan kekurangan. Kelebihan yang dimiliki adalah gratis, memiliki banyak aplikasi dan terkadang memiliki ketahanan terhadap debu dan air. Kekurangan yang dimiliki adalah memori yang terbatas, daya proses yang terbatas, konektivitas yang terbatas, dan masa hidup yang pendek (Lestari, 2014).

Pada android terdapat aplikasi yang dapat membuka file citra sehingga dapat dijadikan sebagai alternatif sementara untuk melihat file citra medis. Namun, file yang disimpan pada android biasanya tidak terenkripsi, sehingga belum memenuhi aspek kerahasiaan dan keamanan file citra medis. Untuk memenuhi aspek kerahasiaan dan keamanan file citra medis yang disimpan pada android, dapat digunakan teknik kriptografi. Dengan teknik kriptografi, file dokumen yang disimpan hanya bisa dibaca atau dilihat oleh orang yang memiliki otoritas untuk membuka file dokumen tersebut.

Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian ilmu dan seni untuk

menjaga suatu pesan atau data informasi agar data tersebut aman. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi (*secrecy*) dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan (*authenticity*) (Wibowo, 2004).

Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. Saat ini, *Advanced Encryption Standard* (AES) merupakan algoritma *cipher* yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh *National Institute of Standard and Technology* (*NIST).* AES menggantikan *Data Encryption Standard* (DES) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit (Wibowo, 2004).

Pada tugas akhir ini akan dikembangkan suatu aplikasi enkripsi file citra medis dengan menggunakan AES yang diharapkan mampu berjalan dengan baik dan efisien pada sumber daya yang ada di android, sehingga penyimpanan file citra medis pada android dapat memenuhi aspek kerahasiaan dan keamanan yang dibutuhkan file citra medis.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana mengimplementasi algoritma AES dalam rancang bangun aplikasi enkripsi file citra medis berbasis android agar file citra medis hanya dapat dilihat oleh orang yang memiliki otoritas untuk melihatnya.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan sebuah aplikasi enkripsi file citra medis pada sistem operasi android

yang menggunakan algoritma AES dalam proses pengenkripsian dan pendekripsiannya. Aplikasi yang dihasilkan dapat digunakan untuk mengenkripsi file citra medis agar hanya dapat dilihat oleh orang yang memiliki otoritas untuk melihatnya.

Adapun manfaat yang diharapkan dari tugas akhir ini adalah aplikasi yang dikembangkan dapat digunakan untuk mengenkripsi file citra medis, sehingga dapat menghasilkan file citra medis yang bersifat rahasia dan aman.

1.4. Ruang Lingkup

Dalam penyusunan tugas akhir ini, diberikan ruang lingkup yang cukup jelas agar pembahasan lebih terarah dan tidak menyimpang dari tujuan penulisan. Aplikasi yang akan dikembangkan adalah aplikasi enkripsi file citra medis berbasis android yang mengimplementasikan algoritma AES pada proses enkripsi dan dekripsi filenya.

1) *Input* dan *Output* berupa file citra medis berekstensi png di tempat penyimpanan *storage default android*.
2) Enkripsi dan dekripsi file citra medis menggunakan algoritma AES-128.
3) Bentuk implementasinya menggunakan bahasa pemrograman *Java Standard Edition* (Java SE).
4) Menggunakan Eclipse dengan *Android Developer Tools* (ADT) plugin untuk penulisan dan kompilasi kode.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam laporan tugas akhir ini terbagi menjadi beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

berisi uraian tentang latar belakang masalah, perumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir

BAB II LANDASAN TEORI

berisi penjelasan singkat konsep–konsep yang mendukung pengembangan aplikasi, meliputi konsep Citra, PSNR (*Peak Signal to Noise Ratio*), Citra

Medis, Android, Kriptografi, AES (*Advanced Encryption Standard*), dan Java SE (*Java Standard Edition*).

BAB III ANALISIS DAN PERANCANGAN

membahas proses pengembangan sistem pada tahap definisi kebutuhan, analisis dan perancangan, dengan hasilnya berupa desain dan rancangan sistem yang akan dikembangkan

BAB IV IMPLEMENTASI DAN PENGUJIAN

membahas proses pengembangan aplikasi dan hasil yang didapat pada tahap implementasi serta menerangkan rincian pengujian aplikasi yang dibangun dengan metode *black box*

BAB V PENUTUP

berisi kesimpulan yang diambil berkaitan dengan aplikasi yang dibangun dan saran untuk pengembangan lebih lanjut.