ANALISIS PERBANDINGAN PERFORMANSI SISTEM KEAMANAN PADA ANDROID MENGGUNAKAN ALGORITMA AES DAN ALGORITMA TWOFISH

Taufik Ardi Susilo[1], Anton Herutomo[2], Hilal Hudan Nuha[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Keamanan data merupakan metode untuk mengamankan data tertentu menggunakan algoritma enkripsi data. Keamanan data ini diperlukan untuk mencegah terjadinya pengambilan data secara illegal, guna melindungi hak kekayaan intelektual pemilik data. Terlebih dalam sistem operasi Android dengan basis open source menjadikan data yang terdapat dalam Android mudah ditemukan dan disebarluaskan secara illegal. Oleh karena itu, tujuan dari tugas akhir ini adalah menerapkan algoritma enkripsi data AES dan Twofish untuk membuat sebuah sistem keamanan pada Android. Dalam tugas akhir ini digunakan dua algoritma enkripsi data yang akan dibandingkan performansinya. Pembandingan dua algoritma ini penting untuk menemukan performansi yang paling optimal yang akan diterapkan pada kasus aplikasi Quran digital menggunakan data gambar. Performansi yang diukur mencakup tingkat kecepatan proses enkripsi data hingga data gambar tersebut muncul untuk di baca pada reader. Dari hasil pengujian yang dilakukan pada aplikasi Quran digital dapat diketahui bahwa penggunaan algoritma AES lebih cepat dibandingkan dengan algoritma Twofish. Sedangkan untuk utilitas memori penggunaan algoritma Twofish lebih sedikit penggunaan memorinya dibandingkan dengan algoritma AES. Sedangkan tingkat keamanan yang dilakukan, didapatkan bahwa pengujian pencocokan kunci pada algoritma AES lebih lama dari pada algoritma Twofish.

Kata Kunci : Keamanan data, Android, Algoritma AES, Algoritma Twofish, Quran Digital.

Abstract

Data security is a method to secure specific data using data encryption algorithms. Security of data is necessary to prevent illegal data collection, in order to protect the intellectual property rights of the owner of the data. Moreover, the Android operating system with open source basis to make the data contained in Android easily found and distributed illegally. Therefore, the aim of this final task is to apply data encryption using AES and Twofish algorithms to create a security system on Android. In this final task used two data encryption algorithms to compare performance. Comparing the two algorithms is important to find the most optimal performance to be applied in the case of digital Quran applications using image data. Performance is measured include levels of data encryption processing speeds up the image data appears to read on the reader. From the results of the tests performed on the application of digital Quran known that the AES algorithm is faster than the Twofish algorithm. As for the memory utility Twofish algorithm uses memory lower than the AES algorithm. While the level of security that is done, it was found that the test of key matching in AES algorithms is longer than the Twofish algorithm.

Keywords : Data security, Android, AES algorithm, Twofish algorithm, Digital Quran.

BAB 1 PENDAHULUAN

1.1. Latar Belakang Masalah

Android merupakan sistem operasi berbasis linux dengan *platform* terbuka atau *open source*. Android dapat dimodifikasi oleh para pengembang sesuai dengan keinginannya. Sistem operasi Android banyak digunakan pada ponsel pintar atau *smartphone*. Android saat ini sangat populer dan menjadi gaya hidup masyarakat perkotaan. Perkembangan Android pada kuarter kedua tahun 2012 menurut *Canalys Estimates* mampu menguasai pasar sebesar 68,1% dari total pengguna *smartphone* diseluruh dunia [2].

Besarnya pengguna Android di dunia menyebabkan aplikasi yang dibutuhkan oleh pengguna mengalami kenaikan permintaan [1]. Aplikasi Android pada umumnya merupakan aplikasi *open source* yang dapat dibuka *source*-nya dengan cara menjadikan perangkat *smartphone* ke dalam status *root*. Data yang dapat diambil dan disebarluaskan lewat media yang lain oleh pengguna dapat merugikan pengembang aplikasi yang melindungi hak cipta atas data yang digunakan. Contoh yang dapat diambil yaitu dalam aplikasi *Ebook* atau *Electronic Book*. Pada aplikasi *Ebook* pengembang tidak ingin data *Ebook*-nya disebarkan secara bebas di media yang lain. Oleh karena itu perlu adanya suatu sistem keamanan dalam rangka melindungi data yang digunakan dalam aplikasi Android.

Sistem keamanan yang saat ini teruji dengan baik dan telah ditetapkan sebagai standard keamanan data adalah dengan metode enkripsi data. Enkripsi data telah berkembang dengan berbagai macam algoritma. *National Institute of Standards and Technology (NIST)* telah menetapkan algoritma *Rijndael* sebagai *Advanced Encryption Standard (AES)* [4]. Oleh karena itu sistem keamanan yang baik adalah dengan menggunakan algoritma enkripsi yang telah teruji dan diakui sebagai standart enkripsi di Dunia.

Untuk mengetahui tingkat optimalnya suatu algoritma keamanan yang diterapkan dalam sistem, maka akan diimplementasikan sistem keamanan

dengan menggunakan dua algoritma yang berbeda. Hal ini dilakukan untuk perbandingan guna mendapatkan hasil yang terbaik. Algoritma berbeda yang akan digunakan yaitu algoritma *Twofish* yang juga masuk ke dalam nominasi dalam penetapan standard keamanan data yang dilakukan oleh *NIST*.

1.2. Perumusan Masalah

Dari latar belakang di atas, dapat dirumuskan beberapa detail permasalahan, yaitu:

a. Bagaimana mengimplementasikan algoritma enkripsi data dengan menggunakan algoritma AES?
b. Bagaimana mengimplementasikan algoritma enkripsi data dengan menggunakan algoritma *Twofish*?
c. Bagaimana hasil performansi yang diperoleh dengan menggunakan algoritma AES dibandingkan dengan algoritma *Twofish*?

1.3. Batasan Masalah

Adapun batasan masalah dalam pengerjaan tugas akhir ini adalah :

a. Kasus yang digunakan adalah aplikasi Quran digital menggunakan *file* gambar yang telah di*download* perbagian dari server aplikasi.
b. Satu *file* gambar memiliki besar maksimal 300 Kb.
c. Enkripsi dilakukan saat *file* gambar diekstrak kemudian masuk ke media penyimpanan.
d. Dekripsi dilakukan saat *file* gambar akan ditampilkan untuk dibaca.
e. Metode pengujian performansi menggunakan kecepatan enkripsi dan dekripsi dari kedua algoritma AES dan *Twofish* serta efisiensi utilitas memori yang digunakan. Selain itu akan diuji waktu yang dibutuhkan untuk mem-*brute force* kunci yang digunakan pada proses dekripsi.
f. Client yang diuji berupa perangkat *handphone* dengan spesifikasi prosesor *dual core* 1,5GHz dan RAM 1GB.

1.4. Tujuan

Tujuan dari penyusunan tugas akhir ini adalah untuk menganalisis dan membandingkan performansi aplikasi yang telah mengimplementasikan sistem keamanan menggunakan algoritma kriptografi AES dan *Twofish* yang diukur dari segi kecepatan, utilitas memori, dan keamanan data yang diuji pada masing-masing proses enkripsi dan dekripsi.

1.5. Hipotesa

Hasil penelitian perbandingan performansi algoritma enkripsi AES *Rijndael* dengan *Twofish* yang diuji pada CPU 32 bit dengan besar *file* 16 hingga 2^{15} *byte* menghasilkan *clock cycle* rata-rata sebesar 26,42 *clock* untuk algoritma AES dan 56,6 *clock* untuk algoritma *Twofish* [8]. Sedangkan penggunaan memori rata-rata *Rijndael* unggul 10 Kb lebih sedikit daripada *Twofish* yang dijalankan pada komputer dengan spesifikasi prosesor *dual core* dengan data sebuah teks [9]. Perbandingan performansi algoritma enkripsi dari penelitian ini dapat diketahui bahwa algoritma AES cocok diimplementasikan dalam aplikasi yang membutuhkan waktu yang cepat,sedangkan algoritma *Twofish* cocok untuk diimplementasikan untuk aplikasi yang membutuhkan efisiensi memori.

Implementasi Sistem keamanan dengan menggunakan algoritma enkripsi AES dan Twofish dapat diimplementasikan pada aplikasi di Android dengan waktu komputasi proses *load* data sedikit lebih lama dibandingkan tanpa diimplementasikan sistem keamanan. Hal ini disebabkan karena terdapat proses tambahan yang digunakan untuk mengamankan pesan yang terdiri dari proses enkripsi dan dekripsi.

1.6. Metodologi Penyelesaian Masalah

Pendekatan sistematis dan metodologi yang akan digunakan untuk pemecahan masalah di atas adalah dengan menggunakan langkah-langkah sebagai berikut:

a. Studi Pustaka dan Literatur

   Pada tahap ini dilakukan pencarian sumber-sumber bacaan yang berhubungan dengan Android, algoritma kriptografi AES dan algoritma kriptografi *Twofish*. Pada sumber bacaan yang berhubungan dengan

Android dapat diperoleh dari forum Android, beberapa paper dari IEEE, paper NIST, jurnal penelitian tentang sistem keamanan, dan lainnya.

b. Analisis Masalah

Pada tahap ini dilakukan analisis masalah berdasarkan studi pustaka dan literatur. Pada tahap ini juga dilakukan peninjauan kembali terhadap setiap metode, model, perancangan, dan hal lain yang dianggap perlu untuk dilengkapi sehingga proses implementasi sesuai dengan yang diharapkan.

c. Perancangan dan Implementasi Sistem

Pada tahap ini dilakukan perancangan aplikasi Android yang akan digunakan sebagai objek penelitian. Perancangan aplikasi ini menggunakan bahasa *Java* dan diimplementasikan pada sistem operasi Android yang digunakan dalam *smartphone*. Setelah perancangan aplikasi dilakukan maka tahap selanjutnya adalah implementasi sistem keamanan dengan menggunakan algoritma kriptografi AES dan algoritma kriptografi *Twofish* untuk mengenkripsi data yang akan diunduh kemudian data tersebut akan didekripsi saat akan dibaca.

d. Testing dan Analisis Hasil

Testing dilakukan dengan melakukan tes performansi dari segi kecepatan pada tiap-tiap proses enkripsi dan dekripsi serta penggunaan memori atau *memory utilization* pada Android. Setelah hasil didapat maka akan dibandingkan dan dianalisa algoritma dengan performansi yang paling optimal untuk diimplementasikan pada kasus aplikasi Quran Digital tersebut.

e. Penyusunan Laporan Tugas Akhir

Membuat dokumentasi dari semua tahapan proses di atas berupa laporan yang berisi tentang dasar teori dan hasil tugas akhir ini.

1.7. Sistematika Penulisan

Penyusunan laporan tugas akhir dilakukan dengan sistematika sebagai berikut :

BAB 1 : Pendahuluan

Materi yang akan dibahas mengenai latar belakang pengambilan topik penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penulisan tugas akhir.

BAB 2 : Tinjauan Pustaka

Pemaparan terhadap teori-teori yang mendukung dan mendasari penulisan tugas akhir ini.

BAB 3 : Perancangan Sistem

Penjelasan rancangan sistem yang akan dibangun, meliputi perancangan sistem keseluruhan, perancangan proses, dan perancangan *user interface* dari sistem.

BAB 4 : Implementasi dan Pembahasan Sistem

Penjelasan mengenai pengujian sistem serta analisa terhadap *output* yang dihasilkan.

BAB 5 : Kesimpulan dan Saran

Pemberian kesimpulan dari permasalahan yang dibahas berdasarkan hasil penelitian dengan tahapan-tahapan yang telah dilakukan pada bab sebelumnya. Selain itu diberikan juga kritik dan saran yang dapat menunjang pengembangan selanjutnya.

BAB 5 KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan analisis dan pengujian terhadap sistem keamanan pada Android menggunakan algoritma AES dan *Twofish* dapat disimpulkan :

1. Penggunaan algoritma AES dan algoritma *Twofish* pada aplikasi menyebabkan adanya tambahan waktu dan tambahan utilitas memori yang digunakan.
2. Dari hasil perbandingan pada kasus uji dapat disimpulkan bahwa algoritma AES memiliki kecepatan yang lebih unggul dibandingkan dengan algoritma *Twofish*. Sedangkan untuk utilitas memori algoritma *Twofish* lebih efisien dibandingkan dengan algoritma AES.
3. Besarnya kecepatan dan utilitas memori dipengaruhi oleh besarnya ukuran *file* di mana semakin besar ukuran *file* maka kecepatan semakin lambat dan utilitas memori semakin bertambah. Selain itu adanya *overhead* juga disebabkan adanya *service* dari aplikasi lain yang menyebabkan *processor* bekerja lebih untuk menangani *service* yang ada.
4. Dari hasil uji keamanan dapat disimpulkan bahwa pengujian pencarian kunci membutuhkan waktu yang sangat besar tergantung dari besarnya kunci yang digunakan dalam algoritma. Hasil uji yang didapat menyatakan bahwa algoritma AES memiliki waktu pencocokan kunci yang lebih lama dari algoritma *Twofish*.

5.2. Saran

Untuk pengembangan keamanan pada aplikasi Android, penulis menyarankan:

1. Implementasi algoritma AES untuk aplikasi Android yang mengutamakan kecepatan pemrosesan data.
2. Implementasi algoritma *Twofish* untuk aplikasi Android yang mengutamakan efisiensi memori yang dibutuhkan.
3. Sebaiknya dicoba mengimplementasikan algoritma enkripsi yang lain yang cocok dengan kebutuhan aplikasi.

DAFTAR PUSTAKA

[1] Androlib. 2012. *Android Market Data Analysis*. http://www.androlib.com/appstats.aspx (Diakses 10 Desember 2012).

[2] Canalys. 2012. *Stellar growth sees China take 27% of global smart phone shipments, powered by domestic vendors*. Press Release 2012/081: Shanghai.

[3] Manurung, dan Midian Rahmat Syahputra. 2011, *Laporan Tugas Akhir Analisis Kerahasiaan Data Pada Algoritma Twofish dalam Sistem Pengamanan Data*. Universitas Sumatera Utara: Sumatera Utara.

[4] NIST. 2001. *Announcing The Advanced Encryption Standard (AES)*. Federal Information Standards Publication 197: United State of America.

[5] Nugraha, Riyanda. 2011. *Laporan Tugas Akhir Implementasi Algoritma Rijndael (AES) dengan Metode Pertukaran Kunci Diffi-Hellman untuk Penanganan Pesan pada Instant Messaging*. Institut Teknologi Telkom: Bandung.

[6] Rodiyansyah, Fajar. 2011. *Arsitektur Sistem Operasi Android*. http://educnology.web.id/2011/11/arsitektur-sistem-operasi-android (Diakses pada 9 Agustus 2012).

[7] Sabdacom. 2012. *Sejarah Android*. http://lenterakecil.com/penulisan-daftar-pustaka-dari-internet (Diakses pada 9 Agustus 2012).

[8] Schneier, Bruce, dkk. 1999. *Performance Comparison of the AES Submissions*. NIST: USA.

[9] Setiawan, Willy. *Analisa dan Perbandingan Algoritma Twofish dan Rijndael*. Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung: Bandung.