PERANCANGAN SISTEM MANAJEMEN AKSES DATABASE SQLITE DENGAN AES

Skripsi

oleh
DIONISIUS RIZKY PUTRA W.
71130071

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2017

PERANCANGAN SISTEM MANAJEMEN AKSES DATABASE SQLITE DENGAN AES

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

DIONISIUS RIZKY PUTRA W.
71130071

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2017

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PERANCANGAN SISTEM MANAJEMEN AKSES DATABASE SQLITE DENGAN AES

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 20 April 2017

DIONISIUS RIZKY PUTRA W.
71130071

iii

HALAMAN PERSETUJUAN

Judul Skripsi	:	PERANCANGAN SISTEM MANAJEMEN AKSES DATABASE SQLITE DENGAN AES
Nama Mahasiswa	:	DIONISIUS RIZKY PUTRA W.
N I M	:	71130071
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2016/2017

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 3 Maret 2017

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Lukas Chrisantyo, S.Kom., M.Eng.

iv

HALAMAN PENGESAHAN

PERANCANGAN SISTEM MANAJEMEN AKSES DATABASE SQLITE DENGAN AES

Oleh: DIONISIUS RIZKY PUTRA W. / 71130071

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 16 Maret 2017

Yogyakarta, 11 April 2017
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Lukas Chrisantyo, S.Kom., M.Eng.
3. Sri Suwarno, Dr. Ir. M.Eng.
4. Ignatia Dhian E.K.R, S.Kom, M.Eng

Dekan	Ketua Program Studi
(Budi Susanto, S.Kom., M.T.)	(Gloria Virginia, Ph.D.)

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa yang telah memberi berkah dan perlindunganNya sehingga penulis dapat menyelesaikan laporan penelitian Perancangan Sistem Manajemen Akses Database SQLite dengan AES. Penulisan skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan jenjang perkuliahan Strata I Universitas Kristen Duta Wacana.

Dalam penulisan skripsi ini tentunya tidak lepas dari kekurangan, baik dari aspek kualitas maupun kuantitas materi penelitian yang disajikan. Penulis menyadari bahwa skripsi ini jauh dari sempurna sehingga penulis membutuhkan kritik dan saran yang bersifat membangun untuk perkembangan penulis di masa mendatang.

Pada kesempatan ini penulis dengan tulus hati mengucapkan terima kasih kepada:

1. Bapak Willy Sudiarto Raharjo, S.Kom, M.Cs selaku Dosen Pembimbing I
2. Bapak Lukas Chrisantyo, S.Kom, M.Eng selaku Dosen Pembimbing II
3. Rekan-rekan dan orang tua penulis yang telah membantu penulis dalam berbagai aspek.

Akhir kata, semoga penelitian ini dapat berguna bagi kemajuan pendidikan dan kepentingan masyarakat luas.

Yogyakarta, Maret 2017

Penulis

INTISARI

Perancangan Sistem Manajemen Akses Database SQLite dengan AES

Dalam pembuatan sebuah sistem, peran sebuah *database* sangatlah penting. Salah satu *database* ini adalah SQLite. SQLite ini adalah *database* yang disimpan secara lokal, berbeda dengan *database* lain yang biasanya disimpan dalam server. *File database* ini dapat dibuka dan diubah isinya dengan mudah, sehingga dapat menyebabkan hal-hal yang tidak diinginkan. Hal ini dapat dihindari dengan cara mengamankan *database* tersebut sehingga orang awam tidak dapat mengubah isinya.

Penelitian ini dilakukan untuk mengamankan *database* SQLite tersebut dengan *Access Control List* untuk mengatur akses data antar user dan melakukan enkripsi pada data yang tersimpan. Enkripsi dilakukan dengan menggunakan algoritma AES (*Advanced Encryption Standard*) yang menggunakan *Synthetic IV* (*Initialization Vector*). Dengan cara ini, diharapkan *database* dapat teramankan dan dapat digunakan dengan normal.

Hasil penelitian yang didapatkan ternyata kurang sesuai dengan yang diharapkan karena waktu yang digunakan untuk pemrosesan meningkat tajam, meskipun fungsi manajemen aksesnya berjalan dengan baik. Sistem akan berjalan dengan lebih cepat apabila enkripsi dan *Access Control List* tidak digabungkan (hanya menggunakan salah satu dari keduanya)

Kata kunci: Sistem manajemen akses, *Access Control List (AES),* Enkripsi, Dekripsi, *Advanced Encryption Standard (AES), SQLite*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Perancangan Sistem Manajemen Akses Database SQLite dengan AES

Dalam pembuatan sebuah sistem, peran sebuah *database* sangatlah penting. Salah satu *database* ini adalah SQLite. SQLite ini adalah *database* yang disimpan secara lokal, berbeda dengan *database* lain yang biasanya disimpan dalam server. *File database* ini dapat dibuka dan diubah isinya dengan mudah, sehingga dapat menyebabkan hal-hal yang tidak diinginkan. Hal ini dapat dihindari dengan cara mengamankan *database* tersebut sehingga orang awam tidak dapat mengubah isinya.

Penelitian ini dilakukan untuk mengamankan *database* SQLite tersebut dengan *Access Control List* untuk mengatur akses data antar user dan melakukan enkripsi pada data yang tersimpan. Enkripsi dilakukan dengan menggunakan algoritma AES (*Advanced Encryption Standard*) yang menggunakan *Synthetic IV* (*Initialization Vector*). Dengan cara ini, diharapkan *database* dapat teramankan dan dapat digunakan dengan normal.

Hasil penelitian yang didapatkan ternyata kurang sesuai dengan yang diharapkan karena waktu yang digunakan untuk pemrosesan meningkat tajam, meskipun fungsi manajemen aksesnya berjalan dengan baik. Sistem akan berjalan dengan lebih cepat apabila enkripsi dan *Access Control List* tidak digabungkan (hanya menggunakan salah satu dari keduanya)

Kata kunci: Sistem manajemen akses, *Access Control List (AES),* Enkripsi, Dekripsi, *Advanced Encryption Standard (AES), SQLite*

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Dalam pembuatan sebuah sistem, peran sebuah *database* sangatlah penting. Database berfungsi untuk menyimpan data-data yang terdapat dalam sistem tersebut. Terdapat 2 jenis *database*, yaitu *client-server database* dimana *database* berada pada *server*, dan *embedded database* yang menyimpan data di *local storage*.

Salah satu *embedded database* yang populer adalah SQLite. SQLite banyak digunakan pada aplikasi *mobile*, seperti Android, iOS, dan Windows 10 (Mutti, 2015). SQLite akan membuat *file* yang biasanya berekstensi .db untuk menyimpan data-data tersebut pada *local storage*.

File .db tersebut tidak dienkrip, sehingga pengguna dapat membuka file tersebut dan mengganti isinya. Untuk itulah, sebaiknya file tersebut diamankan dengan cara dienkrip (*encrypt*). Enkripsi adalah suatu metode dimana suatu informasi dirubah sedemikian rupa sehingga hanya pihak-pihak yang berkepentingan saja yang dapat membaca atau mengubahnya.

Selain dienkrip, keamanan pada *database* SQLite tersebut dapat ditingkatkan lebih jauh dengan menambahkan fitur *ACL (Access Control List)* (Mutti, 2015). Dengan fitur ini, *database* SQLite dapat memberikan otoritas untuk bagian-bagian tertentu dalam *database* kepada pihak yang berkepentingan.

Dalam penelitian ini, akan digunakan enkripsi AES untuk mengamankan *database* SQLite. Enkripsi akan dilakukan terhadap *record* yang akan diterapkan proses CRUD (*Create, Read, Update, Delete)* ke dalam *database*. Enkripsi AES masih belum dapat dipecahkan, dan membutuhkan waktu yang sangat lama untuk dapat dipecahkan secara *brute force* (Selent, 2010).

1.2. Rumusan Masalah

Dalam penelitian ini, terdapat beberapa hal yang menjadi pertanyaan penelitian. Hal-hal tersebut adalah:

1. Bagaimanakah kompatibilitas dari *library* yang dibuat pada suatu aplikasi?
2. Seberapa besar penurunan performa aplikasi ketika *library* sudah diimplementasikan?

1.3. Batasan Masalah

Dalam penelitian ini, akan diberikan beberapa batasan masalah yang adalah sebagai berikut:

1. Database yang digunakan adalah SQLite.
2. Metode enkripsi yang digunakan adalah AES-128, AES-192, dan AES-256.
3. Hasil dari penelitian ini hanya akan berupa *library* yang dapat digunakan oleh aplikasi lain.
4. Enkripsi hanya akan dilakukan terhadap *record* yang akan diterapkan CRUD ke dalam *database.*

1.4.Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk merancang sebuah sistem manajemen akses untuk *database* SQLite menggunakan enkripsi AES, yang kemudian diimplementasikan ke dalam sebuah aplikasi dan dianalisa kecepatan kinerjanya.

1.5. Metode Penelitian

Metode yang digunakan dalam penelitian ini antara lain sebagai berikut:

1. Pengamatan Objek

   Pada tahap ini dilakukan pengamatan terhadap objek yang adalah *database* SQLite. Hal-hal yang diamati adalah bagaimana karakteristik *database* SQLite, dan cara kerjanya dalam menyimpan data (CRUD).

2. Perancangan Sistem

   Sistem akan dikembangkan dengan menggunakan AES sebagai algoritma untuk enkripsi dan dekripsinya. Teknik *Access Control List* pun akan diimplementasikan kedalam sistem.

3. Evaluasi

   Evaluasi akan dilakukan dalam dua tahap:

   - Evaluasi dalam pembuatan sebuah aplikasi

     Karena sistem berbentuk sebuah *library* Java, maka akan dibuat sebuah aplikasi sederhana untuk menguji kinerja sistem. Aplikasi ini akan dibangun lalu dianalisa apakah hasilnya seperti yang diharapkan.

   - Menganalisa Performa Sistem

     Sistem akan diuji dengan menggunakan *dummy data* yang akan di CRUD kan ke dalam *database* yang telah dibuat. Metriks yang akan digunakan adalah waktu pemrosesan.

1.6. Sistematika Penulisan

Dalam penulisan penelitian ini, penulis akan membagi laporan ini menjadi 5 bab, yaitu Bab 1 Pendahuluan, Bab 2 Tinjauan Pustaka, Bab 3 Analisis dan Perancangan Program, Bab 4 Implementasi Program dan Evaluasi, dan Bab 5 Kesimpulan dan Saran.

Bab 1 berisi pendahuluan terhadap penelitian, antara lain latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, metode penelitian yang digunakan, dan sistematika penulisan.

Bab 2 berisi tentang tinjauan pustaka serta landasan teori yang digunakan untuk membantu menyelesaikan penelitian ini.

Bab 3 berisi analisis dan rancangan dari program yang akan dibuat, yang berlandaskan dari teori-teori yang telah dianalisis sebelumnya.

Bab 4 berisi penggunaan program serta hasil-hasil yang didapat dari pengujian-pengujian ynag dilakukan.

Bab 5 berisi kesimpulan dari hasil yang telah didapat, dan saran yang bersifat membangun untuk pembaca.

BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil implementasi dan analisis yang telah dilakukan dan dibahas pada bab sebelumnya, dapat disimpulkan bahwa:

1. Fungsi-fungsi dari sistem sudah dapat berjalan dengan baik pada aplikasi pengujian. Hasil dari penelitian ini adalah sebuah *library* yang berbasiskan Java yang berformat .jar.
2. Terjadi penurunan performa secara signifikan ketika data yang digunakan berukuran besar. Hal ini disebabkan oleh karena adanya tabel penampungan sementara dan sistem manajemen akses. Pengecekan akses dilakukan setiap kali proses *select*, *update*, dan *delete* berjalan. Pembuatan *permission* terjadi ketika proses *insert* berjalan, sehingga terdapat dua proses *insert* yang berjalan, yaitu *insert* pada *permission*, dan *insert* pada data itu sendiri. Proses enkripsi dan dekripsi tidak memakan waktu yang cukup signifikan, tetapi menggunakan *memory* yang lebih besar. Perbedaan waktu dan *memory* antara ketiga algoritma enkripsi tidak terlalu besar, hanya selisih sekitar 1 detik.

5.2. Saran

Saran untuk perbaikan dan perkembangan sistem adalah:

1. Mengganti cara dalam menampung data hasil dekripsi untuk menghindari penurunan performa yang tajam.
2. Mengatasi masalah manajemen kunci.
3. Menggunakan AES-256 sebagai algoritma enkripsi karena penalti performa dan waktunya sangat kecil jika dibandingkan dengan algoritma lainnya.

DAFTAR PUSTAKA

Al-Hazaimeh, O. M. (2013). A New Approach for Complex Encrypting and Decrypting Data. International journal of Computer Networks & Communications, 5(2), 95-103. doi:10.5121/ijcnc.2013.5208

Anderson, R. (2008). Security engineering: A guide to building dependable distributed systems. Indianapolis, IN: Wiley Pub. 51-71.

Daemen, J., & Rijmen, V. (2011). The design of Rijndael: AES - the advanced encryption standard. 23-24.

Harkins, D. (2008). Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). doi:10.17487/rfc5297

Liu, H., & Gong, Y. (2013). Analysis and Design on Security of SQLite. Proceedings of the International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013).

Mahajan, Prerna, & Sachdeva, Abhisek. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security.

Mutti, S., Bacis, E., & Paraboschi, S. (2015). SeSQLite: Security Enhanced SQLite. Proceedings of the 31st Annual Computer Security Applications Conference on - ACSAC 2015.

Selent, Douglas. (2010). Advanced Encryption Standard. Rivier Academic Journal.