ISSN 1411-0865

INFOMATEK

Volume 15 Nomor : 1 Juni 2013

JURNAL INFORMATIKA, MANAJEMEN DAN TEKNOLOGI

METODE ANALISIS HIRARKI PROSES (AHP) DALAM PEMILIHAN ALTERNATIF SISTEM PENGOLAHAN AIR MINUM KAWASAN KECAMATAN MARGAHAYU DAN KECAMATAN MARGAASIH KABUPATEN BANDUNG

Sri Wahyuni, Evi Afiatun, Yunita Pusparini

PEMANFAATAN TEKNOLOGI HONEYPOT DALAM MENINGKATKAN AVAILABILITY PADA SISTEM JARINGAN

Doddy Ferdiansyah

STUDI PREFERENSI WISATAWAN DALAM PENERAPAN KONSEP PARKIR JARAK JAUH & LAYANAN ANTAR JEMPUT UNTUK PELAYANAN KAWASAN WISATA BELANJA DI KOTA BANDUNG

Jajan Rohjan, Furi Sari Nurwulandari, Diva Pranatha

PENGARUH CARA BLANCHING DAN PERBANDINGAN ANTARA SUKUN (ARTOCARPUS ALTILIS) DENGAN TEMPE TERHADAP KARAKTERISTIK ABON SUKUN TEMPE

Neneng Suliasih, Yudi Garnida, Fahrunnisa

PENYISIHAN KANDUNGAN BESI (FE) DENGAN MENGGUNAKAN BIOSAND FILTER SKALA RUMAH TANGGA

Lili Mulyatna, Evi Afiatun, Yogi Hermawan

PENERAPAN KEAMANAN DATABASE DENGAN TRANSPARENT DATA ENCRYPTION MENGGUNAKAN SQL SERVER 2008

Rita Rijayanti

Jurnal INFOMATEK	Vol. 15	No. 1	Hal. 1 – 58	Bandung Juni 2013	ISSN 1411-0865

FAKULTAS TEKNIK UNIVERSITAS PASUNDAN BANDUNG

TELAH TERAKREDITASI BERDASARKAN SURAT KEPUTUSAN
DIRJEN DIKTI DEPDIKNAS RI NO. 34/DIKTI/Kep/2003

ISSN 1411-0865

INFOMATEK

Volume 15 Nomor 1 Juni 2013 JURNAL INFORMATIKA, MANAJEMEN DAN TEKNOLOGI

Penerbit : Jurnal INFOMATEK - Informatika, Manajemen dan Teknologi - diterbitkan oleh Fakultas Teknik Universitas Pasundan Bandung

Penerbitan : Frekuensi terbit INFOMATEK dalam satu volume sebanyak 2 nomor per tahun pada setiap bulan : Juni dan Desember. Penerbitan perdana Volume 1 nomor 1 dimulai pada bulan Juni 1999.

Alamat Penyunting dan Tata Usaha : Fakultas Teknik Universitas Pasundan Jl. Dr. Setiabudhi No. 193 Bandung 40153, Tel. (022) 2019435,HUNTING 2019433, 2019407 Fax. (022) 2019329, *E-mail* : infomatek_ft@yahoo.com

ISSN 1411-0865

KEBIJAKAN REDAKSI

1. UMUM

Kontribusi artikel dapat diterima dari berbagai institusi pendidikan maupun penelitian atau sejenis dalam bidang informatika, manajemen dan teknologi. Manuskrip dapat dialamatkan kepada redaksi :

Dr. Bonita Anjarsari, Ir., M.Sc
Jurusan Teknologi Pangan
Fakultas Teknik – Universitas Pasundan
Jl. Dr. Setiabudhi No. 193
Bandung 40153

Manuskrip harus dimasukkan dalam sebuah amplop ukuran A4 dan dilengkapi dengan judul artikel, alamat korepondensi penulis beserta nomor telepon/fax, dan jika ada alamat e-mail. Bahasa yang digunakan dalam artikel lebih diutamakan bahasa Indonesia. Bahasa Inggris, khusus untuk bahasa asing, akan dipertimbangkan oleh redaksi.

2. ELEKTRONIK MANUSKRIP

Penulis harus mengirimkan manuskrip akhir dan salinannya dalam disket (3,5" HD) kepada alamat di atas, dengan mengikuti kondisi sebagai berikut :

a. Hanya mengirimkan manuskrip dalam bentuk 'hard copy' saja pada pengiriman pertama,
b. Jika manuskrip terkirim telah diperiksa oleh tim redaksi, dan 'Redaktur Ahli' untuk kemudian telah diperbaiki oleh penulis, kirimkan sebuah disket (3,5" HD) yang berisi salinan manuskrip akhir beserta 'hard copy'nya. Antara salinan manuskrip dalam disket dan hard copy nya harus sama,
c. Gunakan word for windows '98, IBM compatible PC sebagai media penulisan,
d. Manuskrip harus mengikuti aturan penulisan jurnal yang ditetapkan seperti di bawah ini,
e. Persiapkan 'back-up' salinan di dalam disket sebagai pengamanan.

3. PENGETIKAN MANUSKRIP

a. Pada halaman pertama dari manuskrip harus berisi informasi sebagai berikut : (I) judul, (ii) nama dan institusi penulis, (iii) abstrak yang tidak boleh lebih dari 75 kata, diikuti oleh kata kunci yang berisi maksimum 8 kata, (iv) sebuah catatan kaki dengan simbol bintang (*) pada halaman pertama ini berisi nomor telepon, fax maupun e-mail penulis sebagai alamat yang dapat dihubungi oleh pembaca.
b. Setiap paragrap baru harus dimulai pada sisi paling kiri dengan jarak satu setengah spasi. Semua bagian dalam manuskrip (antara abstrak, teks, gambar, tabel dan daftar rujukan) berjarak dua spasi. Gunakan garis bawah untuk definisi Catatan kaki (footnotes) harus dibatasi dalam jumlah dan ukuran, serta tidak harus berisi ekpresi formula matematik.
c. Abstrak harus menjelaskan secara langsung dengan bahasa yang jelas isi daripada manuskrip, tetapi bukan motivasinya. Ia harus menerangkan secara singkat dan jelas prosedur dan hasil, dan juga tidak berisi abreviasi ataupun akronim. Abstrak diketik dalam satu kolom dengan jarak satu spasi.
d. Teks atau isi manuskrip diketik dalam dua kolom dengan jarak antar kolom 0,7 cm dengan ukuran kertas lebar 19,3 cm dan panjang 26,3 cm. Sisi atas dan bawah 3 cm, sisi samping kiri dan kanan 1,7 cm.
e. Setiap sub judul atau bagian diberi nomor urut romawi (seperti I, II, …, dst), diikuti sub-sub judulnya, mulai dari PENDAHULUAN sampai dengan DAFTAR RUJUKAN. Gunakan hurup kapital untuk penulisan sub-judul.
f. Gambar harus ditempatkan pada halaman yang sama dengan teks dan dengan kualitas yang baik serta diberi nama gambar dan nomor urut. Sama halnya untuk tabel.
g. Persamaan harus diketik dengan jelas terutama untuk simbol-simbol yang jarang ditemui. Nomor persamaan harus ditempatkan di sisi sebelah kanan persamaan secara berurutan, seperti (1), (2).
h. Sebutkan hanya referensi yang sesuai dan susun referensi tersebut dalam daftar rujukan yang hanya dan telah disebut dalam teks. Referensi dalam teks harus diindikasikan melalui nomor dalam kurung seperti [2]. Referensi yang disebut pertama kali diberi nama belakang penulisnya diikuti nomor urut referensi, contoh **:** Prihartono [3], untuk kemudian bila disebut kembali, hanya dituliskan nomor urutnya saja [3].
i. Penulisan rujukan dalam daftar rujukan disusun secara lengkap sebagai berikut :

   Sumber dari jurnal ditulis :

   [1] Knowles, J. C., and Reissner, E., (1958), Note on the stress strain relations for thin elastic shells. *Journal of Mathematics and Physic,* **37**, 269-282.

   Sumber dari buku ditulis :

   [2] Carslaw, H. S., and Jaeger, J. C., (1953), *Operational Methods in Applied Mathematics, 2nd edn*. Oxford University Press, London.

j. Urutan penomoran rujukan dalam daftar rujukan disusun berurutan berdasarkan nama pengarang yang terlebih dahulu di sebut dalam manuskrip.
k. Judul manuskrip diketik dengan hurup "Arial" dengan tinggi 12, 9 untuk abstrak, dan 10 untuk isi manuskrip.

ISSN 1411-0865

INFOMATEK

Volume 15 Nomor 1 Juni 2013 JURNAL INFORMATIKA, MANAJEMEN DAN TEKNOLOGI

DAFTAR ISI

Sri Wahyuni, Evi Afiatun, Yunita Pusparini	1 - 10	METODE ANALISIS HIRARKI PROSES (AHP) DALAM PEMILIHAN ALTERNATIF SISTEM PENGOLAHAN AIR MINUM KAWASAN KECAMATAN MARGAHAYU DAN KECAMATAN MARGAASIH KABUPATEN BANDUNG
Doddy Ferdiansyah	11 - 18	PEMANFAATAN TEKNOLOGI HONEYPOT DALAM MENINGKATKAN AVAILABILITY PADA SISTEM JARINGAN
Jajan Rohjan, Furi Sari Nurwulandari, Diva Pranatha	19 - 28	STUDI PREFERENSI WISATAWAN DALAM PENERAPAN KONSEP PARKIR JARAK JAUH & LAYANAN ANTAR JEMPUT UNTUK PELAYANAN KAWASAN WISATA BELANJA DI KOTA BANDUNG
Neneng Suliasih, Yudi Garnida, Fahrunnisa	29 - 38	PENGARUH CARA BLANCHING DAN PERBANDINGAN ANTARA SUKUN (ARTOCARPUS ALTILIS) DENGAN TEMPE TERHADAP KARAKTERISTIK ABON SUKUN TEMPE
Lili Mulyatna, Evi Afiatun, Yogi Hermawan	39 - 48	PENYISIHAN KANDUNGAN BESI (FE) DENGAN MENGGUNAKAN BIOSAND FILTER SKALA RUMAH TANGGA
Rita Rijayanti	49 - 58	PENERAPAN KEAMANAN DATABASE DENGAN TRANSPARENT DATA ENCRYPTION MENGGUNAKAN SQL SERVER 2008

INFOMATEK
Volume 15 Nomor 1 Juni 2013

PENERAPAN KEAMANAN DATABASE DENGAN TRANSPARENT DATA ENCRYPTION MENGGUNAKAN SQL SERVER 2008

Rita Rijayanti[*)]

Program Studi Teknik Informatika
Fakultas Teknik – Universitas Pasundan

Abstrak: Perkembangan teknologi sebagai sarana komunikasi dalam aktivitas sehari-hari sekarang memaksa kita untuk mengoptimalkan pengamanan data dan informasi yang mengalir. Karena risiko yang cukup besar tersebut, maka bila sebuah sistem tidak memfasilitasi diri dengan pengamanan yang cukup, dikhawatirkan dapat menyebabkan kerugian baik secara materil atau imateril. Pengamanan yang dapat dilakukan salah satunya adalah dari sisi basisdata, dimana salah satu teknik yang dapat digunakan adalah dengan mengunakan enkripsi. Saat ini paling tidak ada tiga tipe dasar dari enkripsi, yaitu manual, semi-transparent dan transparent. *Transparent Data Encription* (TDE) adalah salah satu jenis enkripsi yangi bisa dikatakan sebagai kebalikan dari enkripsi manual. Proses enkripsi dan deskripsi dilakukan pada level rendah, secara permanen, kertika semua operasi read/write, sehingga data yang dienkripsi selalu disimpan dalam bentuk enkripsi. Kajian ini akan membahas cara kerja dari TDE menggunakan SQL Server 2008. Dari pembahasan ini dapat dikatahui performansi pengamanan sebuah sistem jika menggunakan teknik TDE, dimana para penyusup akan sulit melakukan pencurian/perusakan data bahkan jika fisiknya yang terambil pun, dikarenakan data yang mengalir sudah mengalami pernyandian dan mudahnya penerapan keamanan dengan teknik TDE.

Kata kunci : Keamanan dan *Transparent Data encryption.*

I. PENDAHULUAN

Perkembangan teknologi sebagai sarana komunikasi dalam aktivitas sehari-hari saat ini, mulai dari mendapatkan informasi sampai dengan proses transaksi, memaksa kita untuk melakukan optimasi pengamanan data dan informasi yang mengalir pada sebuah sistem. Karena efek dari semakin terbukanya aktivitas menggunakan teknologi informasi ini maka banyak sekali kejahatan yang terjadi saat ini berkaitan dengan pencurian ataupun perubahan data, dimana jika data atau aset tersebut sampai jatuh ketangan pihak-pihak yang tidak bertanggung jawab maka dapat menyebabkan kerugian baik secara materil atau pun imateril bagi pemilik data atau aset tersebut.

Terkait dengan hal ini maka salah satu yang perlu menjadi diperhatikan adalah bagaimana mengamankan data tersebut sehingga dapat membantu menghambat atau bahkan menghilangkan kemungkinan pencurian

[*)] rita.rijayanti@unpas.ac.id

ataupun perubahan data tersebut. Banyak hal yang dapat dilakukan seperti pengamanan dari sisi sistem, basisdata, bahkan infrastuktur. Pada penelitian ini penulis akan mencoba melakukan penerapan keamanan dari sisi basisdata dengan menggunakan teknik enkripsi.

II. LANDASAN TEORI

2.1 Aspek Keamanan

Ketika membahas mengenai keamanan maka tidak akan pernah lepas dari yang namanya aspek keamanan. Berikut adalah beberapa aspek keamanan terkait dengan keamanan[3]:

- *Confidentiality*
  Terkait dengan tindakan pencegahan akses dari pihak-pihak yang tidak berhak melakukan pengaksesan terhadap informasi, umumnya terkait dengan pemberian informasi kepihak lain.
- *Integrity*
  Terkait dengan jaminan kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan perubahan informasi dengan kata lain menjamin keaslian sebuah informasi (utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak).
- *Availability*
  Terkait dengan jaminan pengguna dapat melakukan pengaksesan informasi kapanpun tanpa adanya gangguan. Pengguna dalam hal ini bisa jadi manusia, atau komputer yang tentunya memiliki otorisasi untuk mengakses informasi, umumnya berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- *Authentication*
  Penerima informasi dapat memastikan keaslian pesan yang didapat tersebut berasal dari orang yang seharusnya.
- *Authority*
  Informasi yang melalui sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak (penyusup).
- *Privacy*
  Sifatnya lebih ke arah data-data yang privat (pribadi) dari user.

2.2 Metodologi Keamanan Sistem

Terkait dengan metodologi keamanan sistem informasi maka keamanan di bagi menjadi 4 (empat) level, yaitu [6]:

- *Keamanan level 0*
  Keamanan fisik, merupakan keamanan tahap awal dari komputer *security*. Jika keamanan fisik tidak terjaga dengan baik, maka data-data bahkan hardware komputer sendiri tidak dapat diamankan.
- *Keamanan level 1*
  Terdiri dari database, data *security*, keamanan dari PC itu sendiri, *device*, dan aplikasi. Contohnya : jika kita ingin database aman, maka kita harus memperhatikan dahulu apakah aplikasi yang dipakai untuk membuat disain database tersebut merupakan aplikasi yang

sudah diakui keamanannya. Selain itu kita harus memperhatikan sisi lain yaitu data *security*. Data *security* adalah cara mendesain database.

- *Keamanan level 2*
  Network security / keamanan jaringan. Komputer yang terhubung dengan jaringan sangat rawan dalam masalah keamanan, oleh karena itu keamanan level 2 harus dirancang supaya tidak terjadi kebocoran jaringan, akses ilegal yang dapat merusak keamanan data tersebut.
- *Keamanan level 3*
  Information security. Keamanan informasi yang kadang kala tidak begitu diperdulikan oleh administrator, seperti memberikan password ke teman, atau menuliskannya dikertas, maka bisa menjadi sesuatu yang fatal jika informasi tersebut diketahui oleh orang yang tidak bertanggung jawab.
- *Keamanan level 4*
  merupakan keamanan secara keseluruhan dari komputer. Jika level 1 - 3 sudah dapat dikerjakan dengan baik maka otomatis keamanan untuk level 4 suddah terpenuhi.

Dilihat dari metodologi keamanan sistem terdiri dari level 0 – 4 yang harus diamankan, namun dalam penelitian ini, penulis akan mencoba memfokuskan keamanan pada level 1 (satu), yaitu pengamanan dari sisi sistem database atau basisdata dengan cara menerapkan teknik pengkodean data atau enkripsi.

2.3 Enkripsi

Enkripsi merupakan sebuah cara untuk menjadikan data-data atau informasi tidak dapat terbaca oleh pihak-pihak yang tidak berhak atau tidak memiliki hak akses. Tujuan utama dari enkripsi adalah selain menyembunyikan data/informasi yang terkandung didalamnya juga untuk menjaga intergritas data/informasi pada saat ditransmisikan [5].

Data disandikan (*encripted*) dengan menggunakan sebuah kunci (*key*) dan untuk membuka (*decrypt*) data tersebut digunakan sebuah kunci yang sama dengan kunci untuk mengenskripsi (kasus *private key cryptography*) atau dengan kunci berbeda (kasus *public key cryptography*).

Type dasar dari enkripsi dapat dibagi menjadi [4] :

a. Enkripsi Manual
   Enkripsi tipe ini sepenuhnya dilakukan oleh user dimana user harus memilih secara manual objek mana yang akan di enkripsi dan kemudian menjalankan *command* / perintah khusus untuk melakukan enkripsi dan deskripsi object tersebut.
b. Enkripsi *Semi-Transparant*
   Enkripsi jenis ini disebut juga enkripsi *'On-the-fly'*. Enkripsi ini beroperasi tidak secara permanen, tapi sebelum dan sesudah akses dilakukan pada object-object rahasia atau ketika operasi *read/write*.

c. Enkripsi *Transparent*

Enkripsi ini bisa dikatakan sebagai kebalikan dari enkripsi manual. Proses enkripsi dan deskripsi dilakukan pada level rendah, secara permanen, kertika semua operasi read/write, sehingga data yang dienkripsi selalu disimpan dalam bentuk enkripsi. Dari sisi prinsip-prinsip umum keamanan enkripsi jenis ini adalah tipe yang paling aman dan mudah.

Transparent Data Encryption membuat proses enkripsi sederhana dengan meletakkan enkripsi di dalam database nya sendiri. Dimana aplikasi bisa melanjutkan pekerjaannya tanpa menggunakan database trigger, view, dan aplikasi lain yang digunakan solusi enkripsi database tradisional. Data secara otomatis dienkripsi ketika ditulis pada file database di disk.

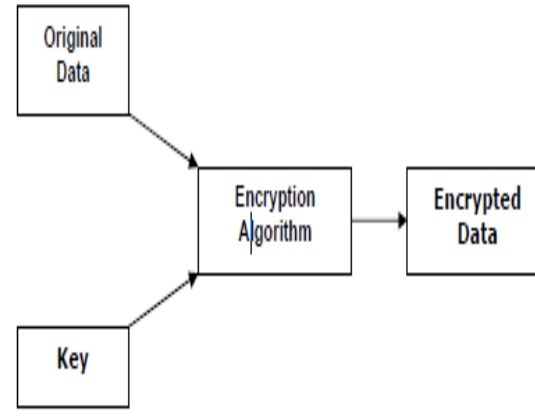
Data secara otomatis di dekripsi untuk semua database user setelah dilakukan autentikasi pada database dan melewati semua pemeriksaan autentikasi tambahan. Tahapan pemeriksaan ini termasuk juga untuk memastikan apakah user mempunyai hak untuk melakukan perintah tertentu (select, update dan delete pada table aplikasi).

Enkripsi Tranparent selain sebagai tindakan pencegahan untuk membantu mengamankan database juga dapat digunakan pada kasus apabila terjadi pencurian pada media fisik / hardware / media backup pada data yang sensitif dilevel sistem operasi.

Proses Enkripsi:

Cara kerja enkripsi dilakukan dengan menambahkan kode karakter teks sumber dengan teks kunci (script sorce code/algoritma). Membandingkan kunci/key yang sudah kita tentukan dengan data sumber dan lakukan perubahan .

Proses dari sebuah enkripsi data dapat dilihat pada gambar 1 [2].

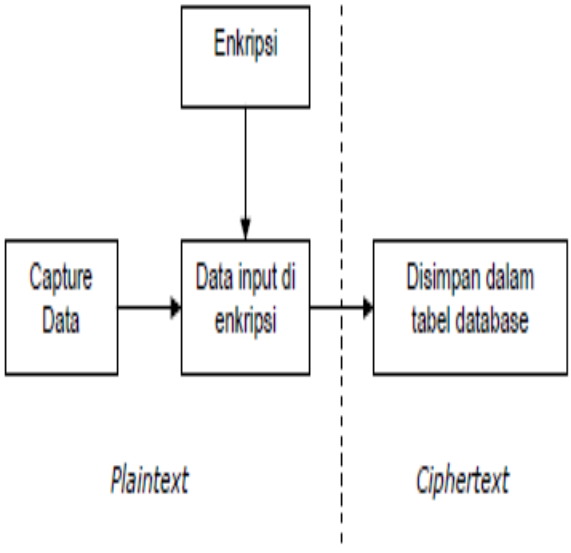


Gambar-1
Proses Encryption Data

Dekripsi adalah kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (*ciphertext*) dikembalikan ke bentuk

aslinya (*Original Plaintext*) sehingga dapat dibaca/ dimengerti kembali.

Proses dari sebuah dekripsi data dapat dilihat pada gambar 2 [2].



Gambar 2

Process Decryption Data

3. HASIL DAN PEMBAHASAN

3.1 Alat dan Bahan Penelitian

Berikut adalah alat dan bahan penelitian yang digunakan dalam menyelesaikan penelitian ini:

(a) Peralatan Software
- Microsoft Windows XP system operasi.
- SQL Server 2008.

(b) Peralatan Hardware
- Notebook Compact Lenovo G480 Core i3.

3.2 Analisis

Pada tahapan analisis ini diperuntukan untuk menunjukan bagaimana penerapan keamanan data base menggunakan konsep *transparent data Encrypsi*.

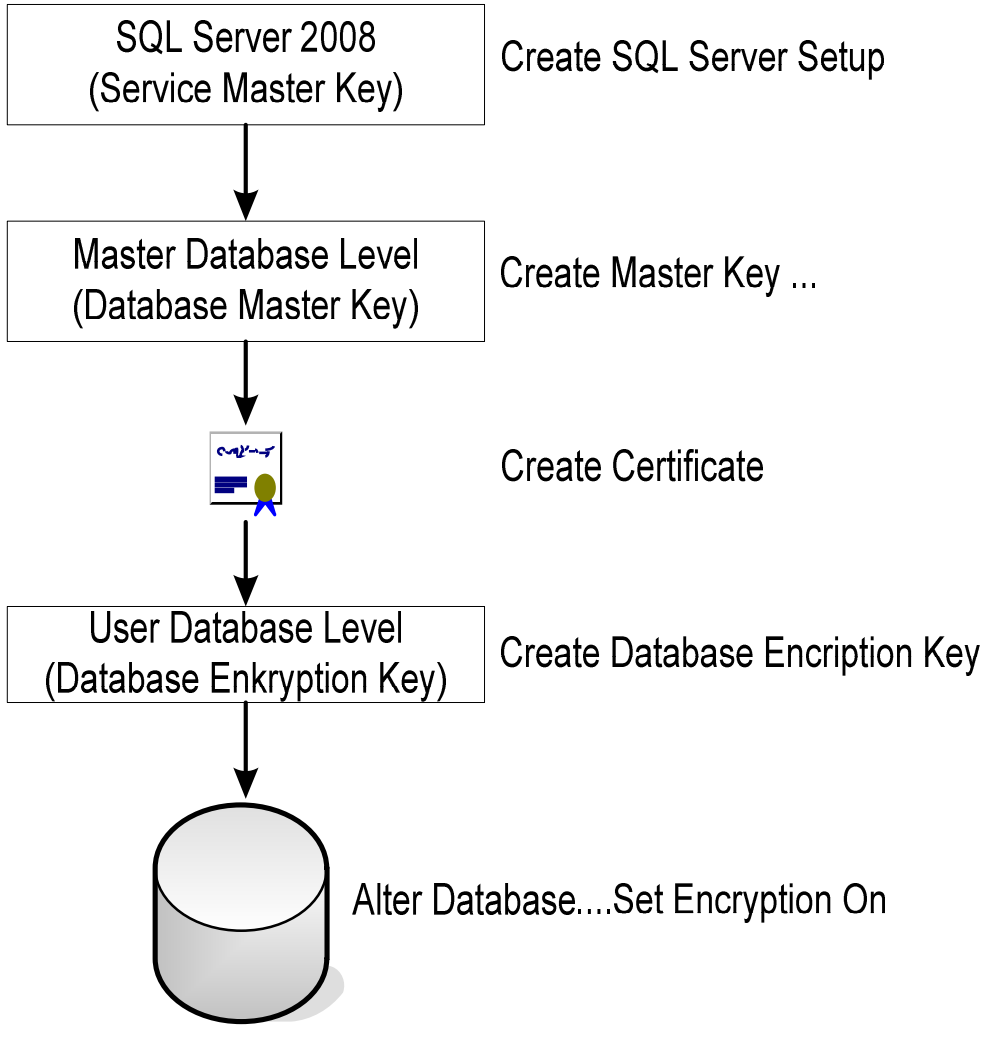
Mekanisme Enkripsi Transparan

Proses *Transparent Data encryption* dengan tools SQL Server 2008 adalah sebagai berikut [1]:

- Membuat Master Key

  Penciptaan Master Key TDE yang diperlukan untuk membuat kunci asimetris sertifikat dan lainnya.

- Membuat Sertifikat TDE
  Sertifikat TDE dinaksudkan untuk keamanan tingkat database.
- Membuat Encryption key
  Script yang digunakan adalah CREATE DATABASE ENCRYPTION KEY <perintah>, sehingga kunci enkripsi tingkat database dapat dihasilkan. Dimana key ini dimaksudkan untuk digunakan pada TDE.
- Aktifkan TDE Encryption Key
  TDE ini tidak akan otomatis aktif, maka harus dilakukan pengaktifan dengan menggunakan script USE <nama database>>;
  SET ENCRYPTION ON



Gambar 3

Transparent Database Encryption Architecture (SQL Server 2008)

3.4 Implementasi Transparent Data Encryption

Penulis akan mencoba melakukan implementasiakan enkripsi menggunakan *Transparent Data Encryption* pada database DBUser yang telah penulis buat sebelumnya, adapun script yang digunakan adalah sebagai berikut:

Script Untuk Membuat Master Key:

```
USE master ;
CREATE MASTER KEY
ENCRYPTION BY PASSWORD = 'MyPassword@1984'
```

Script Untuk Membuat Certificate

```
CREATE CERTIFICATE Cert4DTE
WITH SUBJECT = 'Certificate for TDE'
```

Script Untunk Membuat Database Encryption Key

```
USE DBUser
GO
CREATE DATABASE ENCRYPTION KEY
WITH  ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE Cert4DTE
GO
```

Script Untuk Mengaktifkan TDE

```
ALTER DATABASE DBUser
SET ENCRYPTION ON ;
```

Script untuk melakukan pengecekan status enkripsi:

```
SELECT DB_NAME(database_id), encryption_state,
percent_complete, key_algorithm, key_length FROM
sys.dm_database_encryption_keys ;
```

Results | Messages

	(No column name)	encryption_state	percent_complete	key_algorithm	key_length
1	tempdb	3	0	AES	256
2	DBUser	2	48.17073	AES	256

Gambar 4

Sample Status pengecekan Status Enkripsi

Script Untuk Mendisablekan Enkripsi

```
ALTER DATABASE DBUser
SET ENCRYPTION OFF ;
```

Catatan: Demi keamanan sebaiknya membuat backup untuk sertifikat dan key yang sudah dibuat. Berikut script yang dapat digunakan:

BACKUP CERTIFICATE Cert4DTE TO FILE = 'c:keyexportedCert4DTE'

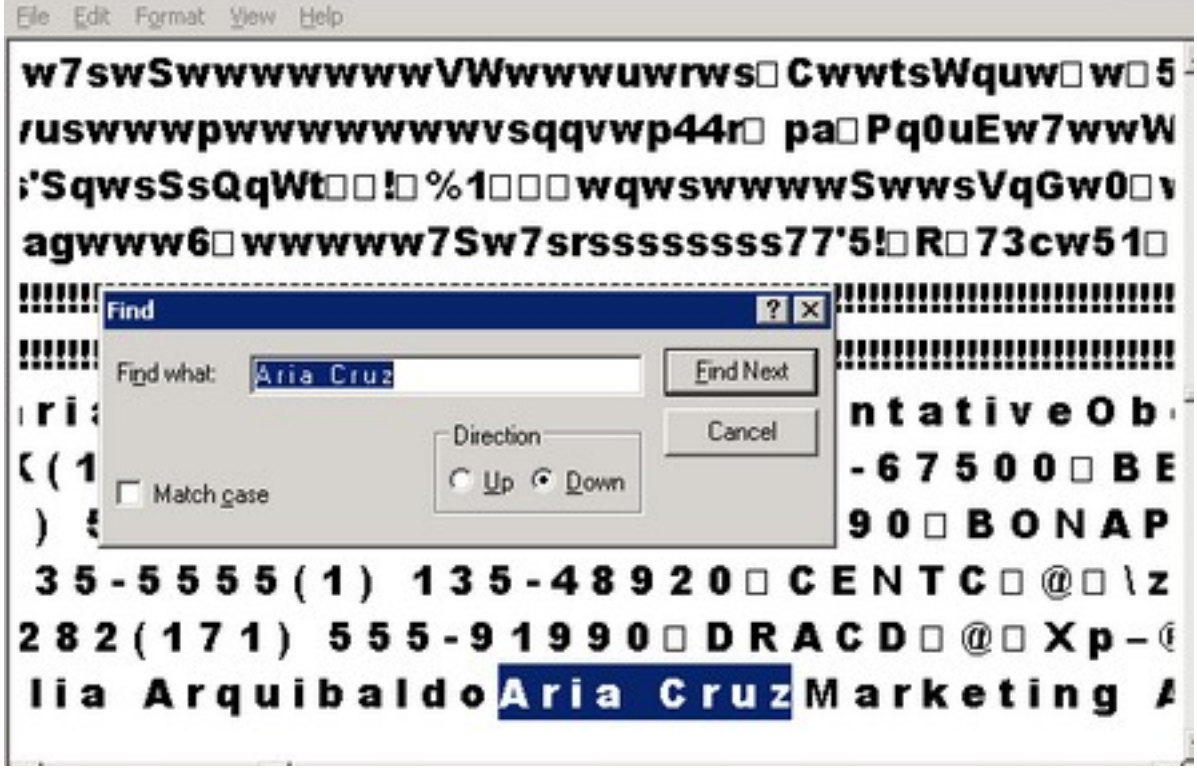
GO

3.5. Perofmansi Transparent Data Encryption

Penulis mencoba melakukan perbandingan paket data sebelum dan sesudah dienkripsi dengan cara membuka backup database dengan menggunakan notepad, kemudian melakukan pencarian data salah satu UserName yang sudah dibuat, sample Username = 'Aria Cruz'.

Sebelum proses TDE

Brikut ini adalah pencarian data sebelum menerapkan teknik DTE, data dapat dengan mudah terbaca.

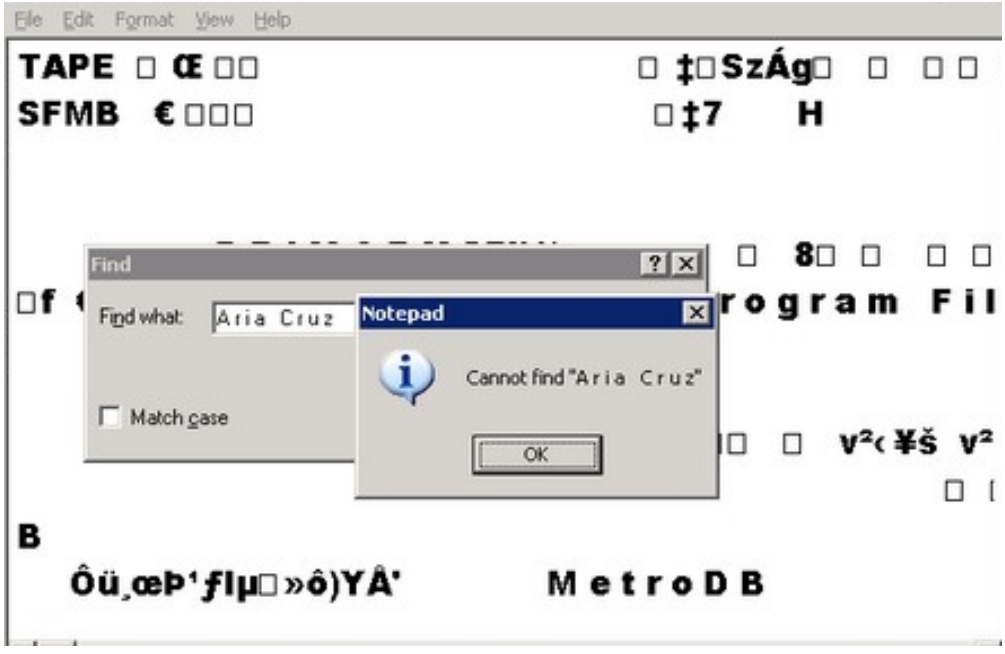


Gambar 5

Sample Pengecekan Status Data Sebelum TDE

Setelah proses TDE

Setelah diterapkan teknik TDE data menjadi tidak dapat terbaca, karena semua data yang ada sudah disandikan dalam bentuk kode. Sehingga dapat terlihat jelas perbedaan dengan jelas hasil data sebelum dan setelah diterapkan teknik TDE.



Gambar 6

Sample Pengecekan Status Data Setelah TDE

3.5 Kesimpulan

Adapun beberapa hal yang dapat disimpulkan dari hasil penelitian ini adalah sebagai berikut :

- TDE merupakan teknik Enkripsi untuk melindungi data/informasi agar tidak bisa terbaca oleh pihak-pihak yang tidak berkepentingan.
- Penerapan TDE pada SQL Server 2008 cukup mudah dilihat dari sisi pengguna, karena hanya cukup melakukan beberapa langkah dalam ekseskusi SQL dan secara otomatis data sudah tersandikan tanpa harus melakukan *coding* dan kompleksitas manajemen key.
- Terkait dengan penerapan dalam sebuah aplikasi, dengan menggunakan TDE maka aplikasi dapat tetap berjalan tanpa perlu adanya database *trigger*, *view* dan perubahan aplikasi lainnya yang diasosiasikan dengan solusi enkripsi database tradisional.
- Kelebihan lainya adalah jika penyerang bermaksud menyerang dan melakukang penyusupan/perusakan pada server yang mempunyai sistem sudah terenkripsi, bahkan jika media fisik tercuri tanpa ada nya key maka pencuri mungkin mendapatkan fisiknya namun data tetap tidak bisa terbaca

tanpa adanya key, seperti yang di coba pada gambar - 5.

4. DAFTAR RUJUKAN

[1] https://msdn.microsoft.com/en-us/library/bb934049.aspx

[2] Rijayanti Rita, 2012, Memaksimalkan Keamanan Sistem Dengan Konsep Encryption dan De-Militaries Zone.

[3] Mesran S.Kom, Diktat:KBMI3523-Keamanan Komputer.

[4] Antonius QWahyu Sudrajat, 2006, Implementasi Enkripsi data base Menggunakan Transparant Data Encription pada Database Engine Oracle

[5] Khafit fauzika, 2011, http://ndolietz.blogspot.com/2011/12/enkripsi-database-menggunakan.html

[6] Keamanan komputer - https://id.wikipedia.org/wiki/Keamanan_komputer