IMPLEMENTASI PENGAMANAN BASIS DATA DENGAN TEKNIK ENKRIPSI

(Studi Kasus: PT. Sugar Group Companies)

Putra Rahmadi[1,] Hilda Dwi Yunita[2]
[1,2]Program Studi S1 Sistem Informasi, Fakultas Komputer-Universitas Mitra Indonesia
Jl. Z.A Pagar Alam No.7 Gedongmeneng Bandar Lampung
[2]hildadwiyunita@umitra.ac.id

ABSTRAK

Pengamanan terhadap jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak – pihak yang langsung berhubungan dengan basis data seperti administrator basis data. Hal ini menyebabkan pengguna basis data harus menemukan cara untuk mengamankan data tanpa campur tangan administrator basis data. Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna basis data membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu. Encryption berasal dari bahasa yunani kryptos yang artinya tersembunyi atau rahasia. Dengan diterapkannya enkripsi maka dapat mengamankan sebuah file data yang merupakan data penting dimana hanya orang tertentu saja yang berhak mengetahui. Hasil penelitian ini menghasilkan dengan adanya program pengaman basis data dengan teknik enkripsi ini mengurangi resiko pencurian data dan kebocoran data ke pihak – pihak luar.

Kata kunci: Enkripsi, Kriptografi, Dekripsi

I. PENDAHULUAN

1.1 Latar Belakang

Berbagai organisasi, perusahaan, atau pun pihak – pihak lain telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data organisasi atau perusahaannya. Seperti PT.SUGAR GROUP COMPANIES saat ini, keamanan terhadap data yang tersimpan dalam basis data sudah menjadi persyaratan mutlak. Pengamanan terhadap jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak – pihak yang langsung berhubungan dengan basis data seperti administrator basis data. Hal ini menyebabkan pengguna basis data harus menemukan cara untuk mengamankan data tanpa campur tangan administrator basis data.

Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna basis data membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Penerapan enkripsi ini akan difokuskan bagaimana enkripsi dapat mengamankan data sampai pada level baris (*row*) dan kolom (*field*) dengan tetap memperhatikan integritas data dan kewenangan setiap pengguna basis data. Algoritma kriptografi yang akan digunakan ialah algoritma kriptografi simetris dan bersifat *stream cipher* sehingga data hasil enkripsi (*cipherteks*) mempunyai ukuran yang sama dengan data asli (*plainteks*). Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi – dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi kunci publik (*asimetris*).

Berdasarkan latar belakang masalah, identifikasi masalahnya adalah penyimpanan data tidak terlalu aman, data dapat dicuri oleh pihak-pihak yang tidak bertanggung jawab.

2. PEMBAHASAN

2.1 Enkripsi

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu. *Encryption* berasal dari bahasa yunani *kryptos* yang artinya tersembunyi atau rahasia.

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Contohnya, *Message* Authentication *Code* (MAC) atau *digital signature*. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer (Saludin Muis, Dr., Ir., M. Kom,2013).

Jenis-jenis enkripsi :
1. ECC (*Elliptic Curve Cryptograph)*
2. *Enkripsi Elgamal*
3. *Diffie-Hellman Key Exchange*
4. RSA
5. *Twofish*
6. AES (*Advanced Encryption Standard*)
7. *Blowfish*
8. Triple DES

2.2 *Kriptografi*

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (*message*). Algoritma kriptografi adalah Aturan untuk enkripsi (*enciphering*) dan dekripsi (*deciphering*). *f*Fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Algoritma kriptografi berkembang terus dan terbagi atas dua bagian yaitu algoritma kriptografi klasik dan modern. Pada kriptografi klasik, kriptografer menggunakan algoritma sederhana, yang memungkinkan *cipherteks* dapat dipecahkan dengan mudah (melalui penggunaan statistik, terkaan, intuisi, dan sebagainya). Algoritma kriptografi modern dibuat sedemikian kompleks sehingga kriptanalis sangat sulit untuk memecahkan *cipherteks* tanpa mengetahui kunci. Algoritma kriptografi modern umumnya beroperasi dalam mode bit. Algoritma ini dapat dikelompokkan menjadi dua kategori yaitu *cipher* aliran (*stream cipher* – beroperasi dalam bentuk bit tunggal) dan *cipher* blok (*block cipher* – beroperasi dalam bentuk blok bit). Pengelompokan algoritma juga dilakukan berdasarkan kunci enkripsi – dekripsi yang digunakan, yaitu simetris (menggunakan kunci yang sama untuk proses enkripsi – dekripsi) dan asimetris atau kunci – publik menggunakan kunci yang berbeda untuk proses enkripsi – dekripsi (Yulianingsih, 2014).

2.3 *Microsoft Visual Studio 2012*

Visual Studio 2012 merupakan salahsatu paket teknologi bahasa pemrograman versi terbaru yang dikeluarkan oleh *Microsoft*. Bahasa pemrograman visual basic digunakan untuk membuat aplikasi windows yang berbasis *Graphical User Interface* (GUI). Micrososft Visual Studio 2012 sebagai produk IDE (*Integrated Develoment Environments*) andalan yang dikeluarkan oleh *Micrososft. Micrososft Visual Studio* 2012 telah menambahkan pembaruan dan perbaikan fitur-fitur untuk melengkapi versi sebelumnya. *Framework* terbaru yaitu *.Net Framework* 4.5 yang merupakan pengembangan sebelumnya dari *.Net Framework* (Wahana Komputer, 2015).

2.4 Kemanan Database

Keamanan database adalah suatu cara untuk melindungi database dari ancaman baik dalam bentuk kesengajaan atau pun tidak.

Keamanan database tidak hanya berkenan dengan data yang ada pada saja, tetapi juga meliputi bagian lain dari *system database*. Agar memiliki suatu keamanan yang efektik dibutuhkan kontrol yang tepat. Seseorang yang mengontrol dan mengatur database adalah administrator, seorang administrator yang memagang peranan penting pada suatu *system database*

2.5 Data

Data adalah fakta dari sesuatu pernyataan yang berasal dari kenyataan, dimana pernyataan tersebut merupakan hasil pengukuran atau pengamatan. Data merupakan komponen dasar dari informasi yang akan diproses lebih lanjut untuk menghasilkan informasi. Berdasarkan pendapat dua ahli tersebut maka penulis menyimpulkan bahwa "Data adalah fakta yang berasal dari kenyataan, yang akan diproses lebih lanjut untuk menghasilkan informasi" (Sutarman 2013).

2.6 UML (*Unified Modelling Language*)

Menurut Rosa dan Shalahuddin (2013), UML adalah bahasa yang banyak digunakan di dunia industri untuk menjelaskan kebutuhan, membuat analisis, desain dan menggambarkan arsitektur dalam pemrograman berorientasi objek.

2.7 Penelitian Terkait

No	Judul	Keterangan
1.	Studi dan implementasi pengamanan basis data menggunakan metode enkripsi md5 (Saipul Bahri, Diana, Susan Dian PS). Jurnal Universitas bina darma (2012)	implementasi pengamanan basis data menggunakan metode enkripsi md5 message-digest algorithm 5 ini dapat diimplementasikan dalam pengamanan basis data khususnya basis data yang berhubungan dengan login ke sistem. Sistem pengamananbasis data ini dibuat menggunakan bahasa pemrograman PHP dan MySQL sebagai databasenya.
2.	Penerapan keamanan basis data denganteknik enkripsi (Hari purwanto). Jurnal Universitas Suryadarma (2016)	Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan. Penerapan kriptografi dapat digunakan untuk mengamankan data dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi,

		dan ketiadaan penyangkalan. Oleh karena itu, pengguna basis data membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya.
3.	Sistem informasi pengamanan basis data menggunakan teknik enkripsi bagian tata usaha lembaga sandi negara (Nunu kustian). Jurnal Univesitas Indraprasta (2014)	Lembaga Sandi Negara sebagai salah satu lembaga pemerintah non-departemen dibentuk karena diperlukannya pelaksanaan tugas pemerintah dibidang persandian sesuai dengan ketentuan peraturan perundang-undangan yang berlaku (keputusan presiden RI nomor 103 tahun 2001. Mengingat bahwa berita rahasia Negara yang dikirim melalui sarana komunikasi perlu dilindungi dari kebocoran-kebocoran, maka penyelenggaraan sistem informasi yang menggunakan teknologi komputer dalam pemberitaan rahasia Negara yang disalurkan dengan sistem persandian,

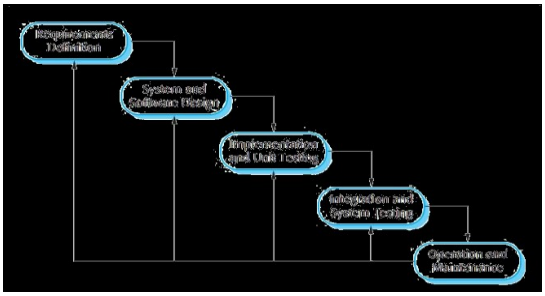
2.8 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan yaitu:

a. Metode *Observasi* (pengamatan), pada metode ini yang dilakukan yaitu melakukan pengamatan terhadap data-data yang akan dikirim secara rahasia atau dienkripsi.
b. Studi pustaka yaitu mencari bahan pendukung dalam penyelesaian masalah melalui buku-buku, paper dan internet yang erat kaitannya dengan masalah yang berkaitan dengan penelitian.

2.9 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan adalah *System Development Live Cycle* (SDLC) dengan pendekatan model *Waterfall*. Model ini bersifat sistematis dan urut dalam membangun sebuah sistem (Rizki, dkk (2014).



Gambar 1. Tahapan SDLC model *Waterfall*

Pengembangan sistem model *waterfall* terdapat beberapa tahapan yaitu: 1) mendefinisi kebutuhan, 2) merancangan sistem dan perangkat lunak, 3) implementasi dan pengujian unit, 4) integrasi dan pengujian sistem, 5) operasi dan pemeliharaan/*maintenance*.

3.3 Metode Perancangan Sistem

Unified Modeling Language (UML*)* menyediakan Sembilan jenis diagram, yang lain menyebutkan delapan karena ada beberapa diagram yang digabung, misalnya diagram komunikasi, diagram urutan dan diagram perwaktuan digabung menjadi diagram interaksi. Namun demikian model-model itu dapat dikelompokan berdasarkan sifatnya yaitu statis dan dinamis. Jenis diagram itu antara lain:

a. *Use Case Diagram*
Use Case Diagram adalah pemodelan untuk kelakuan *(behavior*) sistem informasi yang dibuat dengan kata lain *use case* menjelaskan apa yang dilakukan oleh sistem yang akan dibangun dan siapa yang berinteraksi dengan sistem.

b. *Diagram Activity*
Activity Diagram menggambarkan *wokflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak. (Sukamto dan Shalahuddin (2013 : 161).

c. *Diagram Sequence*
Menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek.

2.10 Metode Pengujian Sistem

Dalam pengujian sistem ini menggunakan *White box* adalah pengujian yang didasarkan pada pengecekan terhadap detail perancangan, menggunakan struktur kontrol dari desain program secara procedural untuk membagi pengujian ke dalam beberapa kasus pengujian. Secara sekilas dapat diambil kesimpulan *white box testing* merupakan petunjuk untuk mendapatkan program yang benar secara 100% (Rosa A.S,M. Shalahuddin 2015).

2.11Analisa Kebutuhan

Dalam penelitian ini akan diuraikan sistem yang dibutuhkan mulai dari spesifikasi komputer yang digunakan untuk merancang program, spesifikasi minimal komputer untuk mengimplementasikan program sampai perangkat

P-ISSN:0216-9436
E-ISSN:2622-6782

lunak (*software*) yang dibutuhkan untuk merancang program dalam penelitian ini.

Kebutuhan Perangkat Keras (*Hardware*)

Dalam perancangan dan pengembangan keamanan basis data dengan teknik Enkripsi ini menggunakan komputer dengan spesifikasi sebagai berikut:

a. Processor Aspire E 11
b. Ram 2 GB
c. Hard Disk 500 GB

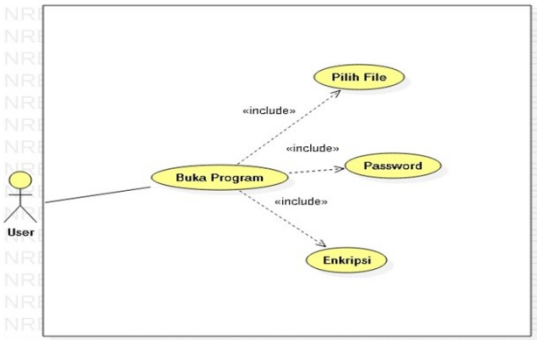
Kebutuhan Perangkat Lunak (*Software*)

Untuk merancang Program keamanan basis data dengan teknik enkripsi ini membutuhkan beberapa Perangkat Lunak (*software*), antara lain :

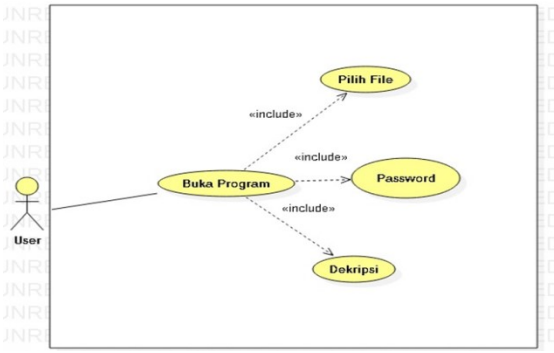
a. Sistem Operasi Windows 7 32-bit
b. Microsoft Visual Studio 2012
c. *StarUML*

Implementasi Pengamanan Basis Data dengan Teknik Enkripsi ini sesuai dengan konsep dan tujuan awal yaitu memberikan pengamanan basis data dalam proses Enkripsi. Implementasi Pengamanan Basis Data dengan Teknik Enkripsi yang dibangun menggunakan sebuah rancangan model UML *(Unified Modeling Language)* seperti *Use Case Diagram, Activity Diagram, Sequence Diagram*.

a. Use Case Diagram
Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi



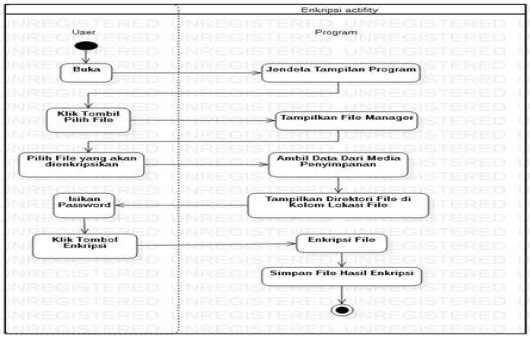
Gambar 2. *Use Case* Enkripsi



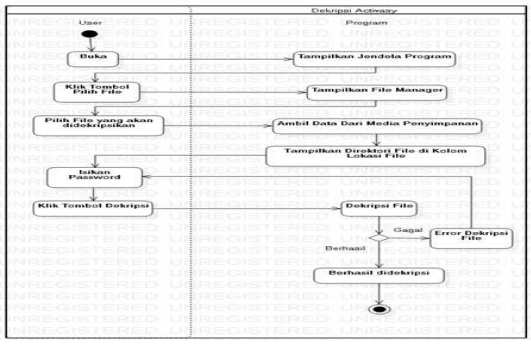
Gambar 3. *Use Case* dekripsi

b. Activity Diagram

Untuk menjelaskan secara detail maka *activaty diagram* dapat dipersentasikan pada Gambar 4 dan Gambar 5.



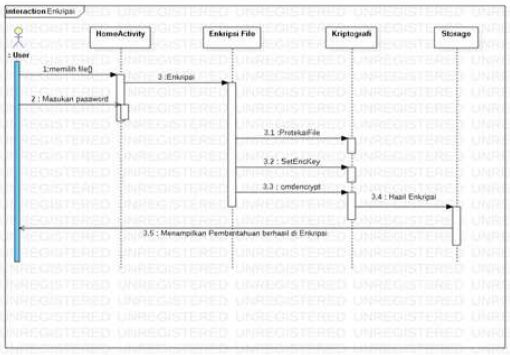
Gambar 4. *Activity diagram* Enkripsi



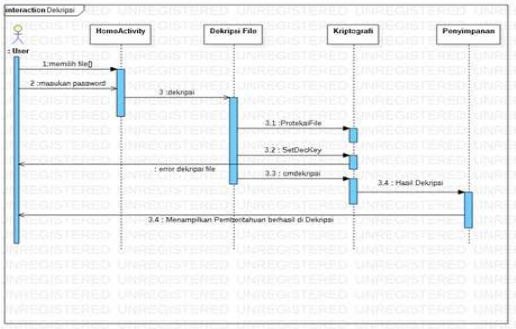
Gambar 5. *Activity diagram* dekripsi

c. Sequence Diagram

Untuk menjelaskan secara detail masing - masing digambarkan pada Gambar 6 dan Gambar 7



Gambar 6. *Sequence diagram* Enkripsi



Gambar 7. *Sequence diagram* dekripsi

P-ISSN:0216-9436
E-ISSN:2622-6782

2.12 Hasil

Penerapan Implementasi Pengamanan Basis Data dengan Teknik Enkripsi ini dapat dijalankan pada berbagai platform sistem oprasi dan perangkat keras, spesifikasi perangkat lunak (*software*) yang digunakana dalah sebagai berikut:

1. Sistem Oprasi Windows 7
2. *Microsoft Visual Studio* 2012
3. *Star UML*

Sedangkan spesifikasi perangkat keras (*hardware*) yang dibutuhkan berdasarkan kebutuhan yang harus terpenuhi antara lain:

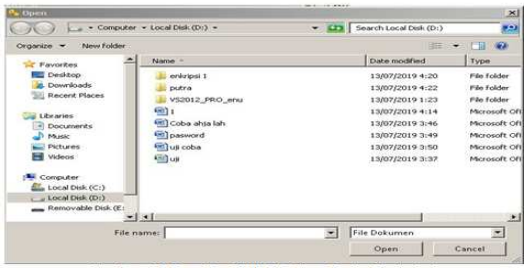
1. Processor Aspire E 11
2. Ram 2 GB
3. Keyboard, mouse, dan monitor sebagai peralatan antarmuka

Hasil Aplikasi

1. Halaman Login

Gambar 8. Tampilan Program Enkripsi dan Dekripsi

2. Tampilan Pilih File yang ingin dienkripsi



Gambar 9. Tampilan Pilih File yang ingin dienkripsi

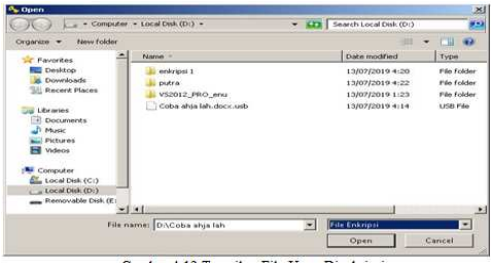
3. Tampilan *Password*

Gambar 10. Tampilan *Password*

4. Tampilan Pesan Box Enkripsi Berhasil

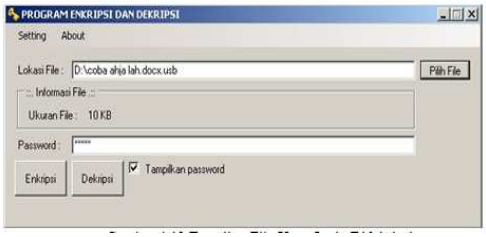
Gambar 10. Tampilan Pesan Box Enkripsi Berhasil

5. Tampilan file hasil enkripsi



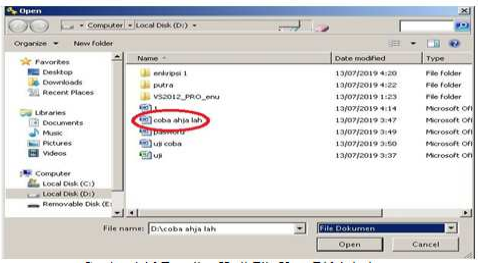
Gambar 11. Tampilan file hasil enkripsi

6. Tampilan Dekripsi



Gambar 12. Tampilan Dekripsi

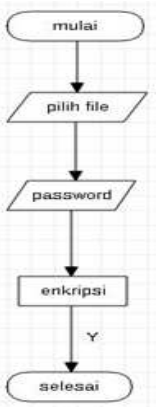
7. Tampilan file hasil Dekripsi



Gambar 13. Tampilan file hasil Dekripsi

Hasil Pengujian

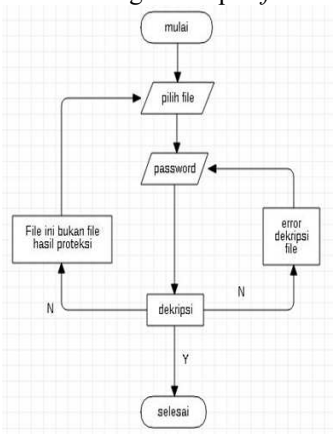
a. Di bawah ini adalah hasil tahapan coding enkripsi di atas dengan tahapan *flowchart diagram.*



Gambar 14. *Flowchart Diagram* Enkripsi

Flowchart di atas diartikan saat pengguna ingin mengenkripsi file langkah awal pengguna harus memilih file yang ingin di ubah selanjutnya pengguna di haruskan memasukan password untuk mengunci file yang ingin dienkripsi dan selanjutnya pengguna harus nengklik tombol enkripsi agar mengenkripsikan file berjalan lalu selesai.

b. Di bawah ini adalah hasil tahapan coding dekripsi di atas dengan tahapan *flowchart diagram.*



Gambar 15. *Flowchart Diagram* dekripsi

Flowchart di atas diartikan saat pengguna ingin mengdekripsikan file yang dienkripsi langkah awal pengguna harus memilih file enkripsi, selanjutnya pengguna di haruskan memasukan *password* yang di gunakan saat enkripsi file, lalu tahapan terakhir klik tombol dekripsi. Jika saat proses dekripsi ada tampilan pemberitahian "file ini bukan file hasil proteksi" pengguna bukan memasukan file hasil enkripsi.

Jika saat proses dekripsi ada tampilan pemberitahian error dekripsi file, pengguna salah memasukan *password* atau *password* tidak sama saat pengenkripsian file.

3. KESIMPULAN

Implementasi keamanan basis data dengan teknik enkripsi merupakan program baru yang akan di gunakan pada PT. Sugar Group Companies yang mana saat ini perusahaan tersebut belum ada program ini untuk keamanan data penting milik perusahaan. Adapun kesimpulan yang dapat diambil dari pembuatan program ini antara lain:

1. Dengan adanya program pengaman basis data dengan teknik enkripsi ini akan memudahkan pemilik PT Sugar Group Companies untuk mengamankan data – data penting dengan dienkripsikan.
2. Dengan adanya program pengaman basis data dengan teknik enkripsi ini mengurangi resiko pencurian data dan kebocoran data ke pihak – pihak luar.

PUSTAKA

Bahri Saipul, Diana, Susan Dian Ps. 2012. Studi Dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi Md5. Palembang. Universitas Bina Darma.

Komputer Wahana. 2015. Membuat Aplikasi Kreatif Dengan Visual Basic .Net 2012. Semarang. CV Andi Offset.

Kustian Nunu. 2014. Sistem Informasi Pengamanan Basis Data Menggunakan Teknik Enkripsi Bagian Tata Usaha Lembaga Sandi Negara. Jakarta. Jurnal Univesitas Indraprasta.

Muis Saludin, Dr., Ir., M. Kom. 2013. Pengantar Kriptografik Kuantum, Teknik
Enkripsi Masa Depan. Jakarta. Graha Ilmu.

Purwanto Hari. 2016. Penerapan Keamanan Basis Data Dengan Teknik Enkripsi. Makasar. Universitas suryadarma.

Rosa A. S and M. Shalahuddin. 2013. Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek, 2nd ed. Bandung, Indonesia: Informatika.

Rizki Alfiasca, Pantjawati, Sudarmaningtyas. 2014. Rancang Bangun Sistem Informasi Manajemen Arsip Rumah Sakit Bedah Surabaya Berbasis
Web. JSIKA Vol 3, No 1. STMIK STIKOM Surabaya

Sutarman. 2013. Pengantar Teknologi Informasi. Yogyakarta: PT Bumi Aksara.

P-ISSN:0216-9436
E-ISSN:2622-6782