IMPLEMENTASI ALGORITMA RC4 DAN KOMPRESI LZW UNTUK PENGAMANAN DATABASE PADA PT. MPP INTERNATIONAL DEVELOPMENT INDONESIA

Abdul Rahman Wahid[1)], Syafrullah[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : rizkiajiwibowo@gmail.com[1)], mohammad.syafrullah@budiluhur.ac.id[2)]

Abstrak

PT. MPP International Development Indonesia yang bergerak dibidang jasa spesialis proyek, struktur bangunan, kontraktor, proyek manager dan konsultan proyek. PT. MPP international Development Indonesia salah satu perusahaan yang sudah betaraf internasional dan jam terbang yang sudah cukup banyak. Ada beberapa perusahaan-perusahaan yang cukup terkenal yang mempercayai PT. MPP International Indonesia untuk membangun daripada gedung-gedung perusahaan contohnya yaitu google, Yahoo, Grand Hyaat Bali, Bakrie Tower, Kedutaan Besar Australia dan Bank China yang ada di Indonesia. PT. MPP International Development Indonesia menjaga baik data para kontraktor agar tidak terjadi kesalahan atau kebocoran data maupun kecurangan rancangan anggaran biaya dalam berbagai tender yang diajukan. Tetapi data tidak akan aman apabila disimpan menjadi bentuk file. Maka oleh dari itu dibutuhkan suatu pemecah masalah dalam mengaman data yang nantinya akan dibaca dan bisa dilihat dengan mudah, yang dimana ini akan dibuat untuk perusahaan yang membutuhkan solusi seperti yang diajukan. Kriptografi yang digunakan dalam pembuatan apikasi keamanan ini ialah RC4 (Rivest Code-4) dan kompresi LZW (Lempel-Ziv-Welch). Dimana didalam aplikasi ini terdapat perhitungan yang lumayan rumit dengan menggunakan kunci yang nantinya akan digunakan untuk mengamankan database yang ada disimpan,

Kata Kunci : Kriptografi, Enkripsi, RC4, LZW, Database, Rancangan Anggaran Biaya

1. PENDAHULUAN

PT. MPP *International Development* Indonesia yang bergerak spesialis proyek, struktur bangunan, kontraktor, proyek *manager* dan konsultan proyek memiliki *database* yang berisi data dokumen kontrak antar *owner* dan konsultan proyek, data *invoices*, dan data gambar struktur.beberapa kali data yang ada didalam database memiliki suatu kesamaan data baik itu type data ataupun isi data tersebut. Dimana nanti ini akan memudahkan user lain dalam menggunakan akses dalam membaca database yang dimana filenya sudah diamankan masih dapat dilihat dengan mudah, baik itu sifatnya dalam pembocoran data, penyadapan ataupun pengeditan data serta penggandaan data terhadap isi dari database tersebut..

Untuk mengatasi masalah-masalah diatas, developer melakukan suatu pengembangan cara dalam merumuskan suatu rumus dalam mengamankan data agar tidak ada penyalah gunaan dalam mengamankan data. Dimana developer menggunakan suatu metode dalam penulisan ataupun pembuatan aplikasi keamanan yang dibuat ialah menggunakan algoritma RC4 dan kompresi LZW yang akan diimplementasikan pada aplikasi kriptografi berbasis *web* untuk mengamankan basis data PT. MPP *International Development* Indonesia.

2. LANDASAN TEORI

2.1 Algoritma *Rivest Code* 4

Algoritma Rivest Code 4 ialah satu dari sekian jenis stream cipher adalah dalam memproses unit atau masukkan data pada suatu wadah tertentu. Dengan metode ini enkripsi dan dekripsi dapat dilakukan pada panjang variable. Algoritma ini tidak mengharuskan user menunggu proses inputan data atau mengupdate byte tambahan lagi untuk dilakukan enkrip data.

Rivest Code 4 adalah algoritma yang menggunakan panjang kunci dari 1 sampai dengan 256 byte dalam menginisialisasi state table. State table sendiri berfungsi dalam mengurutkan dan menghasilkan byte pseudo random yang akan nanti menjadi steam pseudo random. Setelah dimana nanti XOR yang menjadi plainteks akan dirubah menjadi cipherteks. Dimana setiap bagian-bagian atau part-part yang ada pada state table digantikan sedikitnya satu kali pergantian.

2.2 Algoritma Enkripsi RC4

Algoritma Enkripsi Rivest Code 4 adalah jenis stream cipher yang memiliki S-Box, S0, S1, …., S255, yang nanti akan berisi permutasi daru bilangan 0 hingga 255, dan permutasi merupakan kegunaan dari kunci dengan panjang yang variable. "A Hanriyawan (2004)". Dalam algoritma enkripsi metode ini akan membangkitkan pseudo ramdom yang nanti dimana byte dari key akan dihadapkan pada operasi XOR pada plainteks dalam menghasilkan cipherteks.

Secara umum algoritma ini merupakan salah satu bagian dari metode algoritma Rivest Code 4, yang dimana sudah dibagi menjadi 2 yaitu Key Schedulling Algorithm (KSA) dan stream generation atau Pseudo Random Generation Algorithm (PRGA)

a. *Key Setup / Key Schedulling Algorithm*

Key Setup sendiri memiliki beberapa tahap dalam memproses suatu operasi ialah sebagai berikut :

1) Inisialisasi S-Box

Pertama ialah tahap inisialiasasi S-Box yang nanti akan memasukkan data dengan nilai yang telah disesuaikan dengan indeks untuk mendapatkan hasil dari table S-Box.

2) *Key Byte Array*

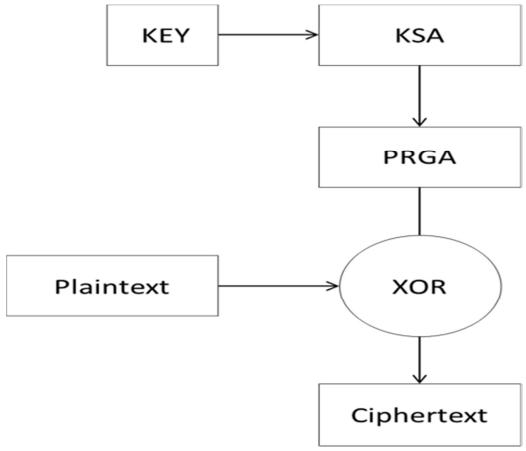
Pada tahap kedua yaitu key byte array ialah dimana kunci akan dapat digunakan untuk melakukan proses enkripsi dan dekripsi yang nanti akan dimasukkan agar array menjadi ukuran maksimal yaitu 255. Secara berulang sampai seluruh array terisi.

3) Perbandingan Sebuah Nilai Dalam Permutasi

Tahap terakhir yang dilakukan ialah tahap perbandingan sebuath nilai dalam permutasi terhadap S-Box. Dimana langkah awal yang dilakukan ialah mengurutkan S(0) = 0, S(1) = 1, …., S(255) = 255. Kemudian isi array 256 byte yang nanti akan dilakukan seperti looping dimana seluruh array seperti array K(0), K(1), …., K(255) terisi selurusnya. Set indeks j dengan nol.

b. *Stream Generation* Atau *Pseudo Random Generation Algorithm* (PRGA)

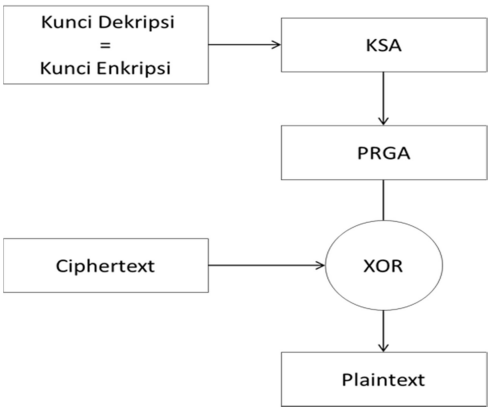
Pada tahapan ini, dimana tahap stream generation atau pseudo random generation algorithm akan menghasilkan suatu pseudo random yang nanti akan dilakukan suatu operasi XOR dalam menghasilkan cipherteks dan juga dapat menghasilkan plainteks. Dimana pada tahap ini ialah merupakan tahap awal pada proses stream generation atau juga bisa disebut pseudo random generation algorithm.



Gambar 2.1 : Arsitektur Enkripsi RC4

2.3 Algoritma Dekripsi RC4

Algoritma dekripsi mirip dengan algoritma enkripsinya, perbedaannya hanya pada saat *stream generation*, yaitu untuk mendapatkan suatu bentuk plainteks dalam bentuk awal, maka cipherteksnya akan dilakukan suatu proses operasi XOR pada pseudo random byte. Algoritma *key setup* pada proses dekripsi sama dengan algoritma enkripsi yang diproses inisialisasi S-Box, penyimpanan kunci dalam *key byte array* hingga proses inisialisasi S-Box berdasarkan *key byte array*. Untuk itu cara dekrips dan enkrip yang dilakukan akan membentuk suatu key stream generation. Yaitu suatu proses yang nanti akan dioperasikan bersama key stream ialah cipherteks yang nanti akan menghasilkan suatu bentuk awal dari proses yang sedang terkadi ialah plainteks. Berikut ini adalah gambar yang menunjukan proses enkripsi dari algoritma RC4:



Gambar 2.2 : Arsitektur Enkripsi RC4

3. ANALISA MASALAH DAN PENYELESAIAN

3.1 Analisa Masalah

Dalam masalah mengamankan data yang ada di PT. MPP *International Development* Indonesia ini memiliki beberapa kendala Kendala yang terjadi adalah sepertinya kebocoran data dan keaslian data yang harus lebih bisa jaga kerahasiaannya.

3.2 Penyelesaian Masalah

Menurut survei dan penulusuran yang sudah dilakukan diddapat penyelesaian masalah yang ada ialah membangun suatu aplikasi yang nanti akan mampu dalam mengamankan data. Aplikasi ini engamankan isi dari *database* pada PT. MPP *International Development* Indonesia supaya informasi yang ada tidak akan mudah untuk diketahui oleh orang luar dan terhindar dari tangan-tangan yang tidak bertanggung jawab. Untuk mewujudkan itu makan developer melakukan terobosan dalam menyelesaikan masalah yang ada pada PT. MPP International Development Indonesia ialah membuat suatu aplikasi keamanan data yang baik dari segi mengamankan data dimana memiliki perhitungan matematika yang rumit , dimana dalam pembuatan aplikasi tersebut digunakan dengan metode algoritma kriptografi RC4 dan kompresi LZW. Dan menghasilkan aplikasi pengamanan *database* berbasis *web* yang *user friendly,* mudah dimengerti dan digunakan oleh pengguna.

4. IMPLEMENTASI DAN UJI COBA PROGRAM

4.1 Implementasi Program

Dalam mengetahui sejauh mana aplikasi keamanan database in dapat membantu mengamankan data yang ada maka akan dilakukan proses implementasi terhadap aplikasi keamanan database yang bersifat *web.* Aplikasi ini dirancang untuk mengamankan data pada datasbase dengan hanya dua *user* yang mendapatkan hak dalam mengakses aplikasi ini. Agar aplikasi yang telah dibuat oleh developer ini menjadi suatu aplikasi yang bermanfaat bagi perusahaan maka development akan menjamin kelancaran dari segala operasi yang dilakukan aplikasi ini dalam mengamankan data yang ada dengan baik. Dan oleh sebab itu maka dibutuhkan suatu beberapa kriteria yang sesuai agar dapat menggunakan aplikasi keamanan ini seperti kebutuhan dari segi perangkat keras dan perangkat lunak.

No	Perangkat	Kebutuhan
1	CPU	Intel Core i7-4210U@1.70GHz
2	Hardisk	1 TB
3	RAM	8.00 GB
4	VGA	NVIDIA GeForce 940M

4.2 Spesifikasi *Hardware* Dan *Software*

Aplikasi Keamanan berbasis *web* ini dibuat menggunakan bahasa pemrograman *php* dan *database* MySQL. Berikut spesifikasi *hardware* dan *software* yang dibutuhkan agar sistem pendukung keputusan berjlan dengan baik.

a. Perangkat Keras

Spesifikasi perangkat keras yang digunakan untuk mengembangkan program dapat dilihat pada tabel berikut:

Tabel 1 : Perangkat Keras

b. Perangkat Lunak

Spesifikasi perangkat keras yang digunakan untuk mengembangkan program dapat dilihat pada table berikut :

No	Perangkat	Kebutuhan
1	Sistem Operasi	Microsoft Windows 10 Pro 64-bit
2	Editor Text	Atom Version 1.23.1
3	Server	XAMPP v 3.2.2

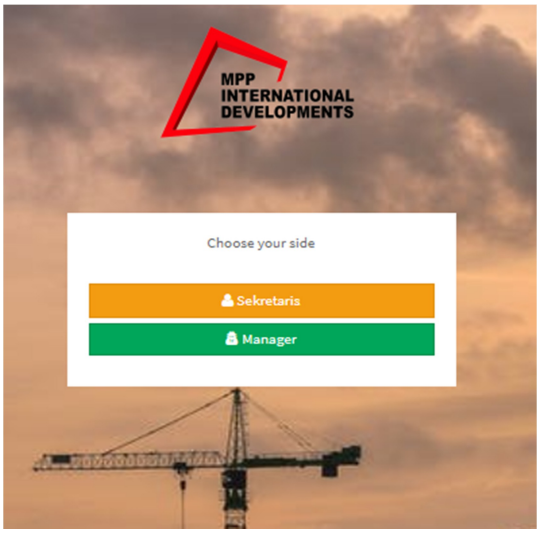
Tabel 2 : Perangkat Lunak

4.3 Uji Coba Program

Pada tahap ini development melakukan suatu uji coba dalam pembuatan aplikasi yang ada. Dimana dalam pembuatan aplikasi ini bertujuan mengamankan data yang ada yang nanti akan disimpan pada database yang sudah ditentukan. Dan aplikasi yang dibuat ialah aplikasi keamanan yang berbasis web yang nanti akan menggunakan suatu bahasa pemograman yang agak sulit tetapi disini developmer melakukan suatu terobosan dalam tampilan yang dibuat lebih menarik dan bagus supaya mudah dibaca dan dilihat.

a. Tampilan Layar *Form* Awal

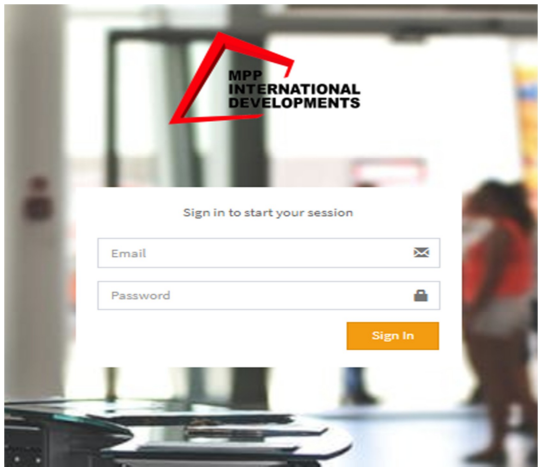
Pada tampilan form awal untuk memilih sign in ke sekretarus atau manager dimana nanti bertujuan untuk masuk ke Menu utama aplikasi dari sekretaris atau manager.. Dalam form awal user hanya diminta memilihh yaitu ingin membuka form sign inn menu sekretaris atau manager.. Bisa dilihat pada gambar berikut.



Gambar 4.1 : Tampilan Layar *Form* Awal

b. Tampilan Layar *Form Sign In* Sekretaris

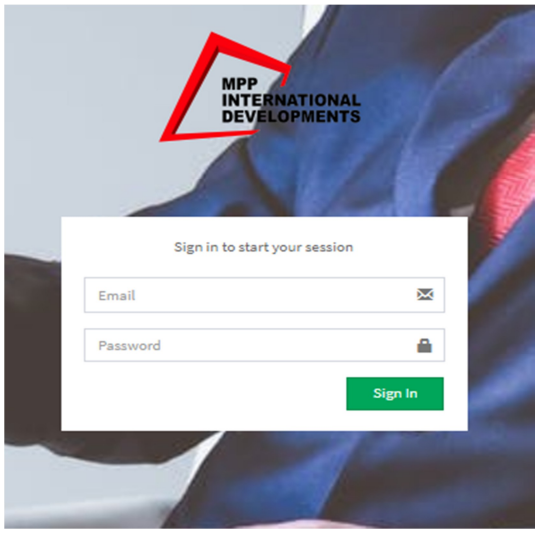
Pada tampilan *form Sign In* Sekretaris seperti yang dapat dilihat, terlihat ada permintaan dalam memasukkan ID user dan Password agar user dalam dengan mudah melakukan akses masuk pada menu utama yang nanti akan terbuka apabila user telah melakukan inputan ID dan Password yang valid. Bisa dilihat pada gambar dibawah ini.



Gambar 4.2 : Tampilan Layar *Form Sign In* Sekretaris

c. Tampilan Layar *Form Sign In Manager*

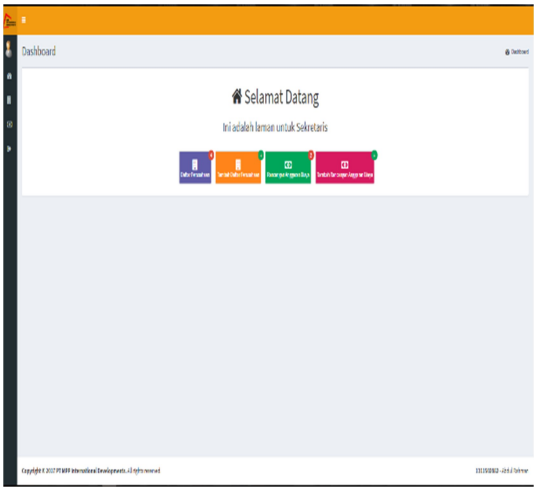
Untuk dapat mengakses *Dashboard Manager* aplikasi maka harus *Sign In* melalui *form Sign In* yang telah disediakan. *Manager* memasukkan *email* dan *password* yang digunakan untuk *Sign In*. Bisa dilihat pada gambar dibawah ini:



Gambar 4.3 : Tampilan Layar *Form Sign In Manager*

d. Tampilan Layar *Dashboard* Sekretaris

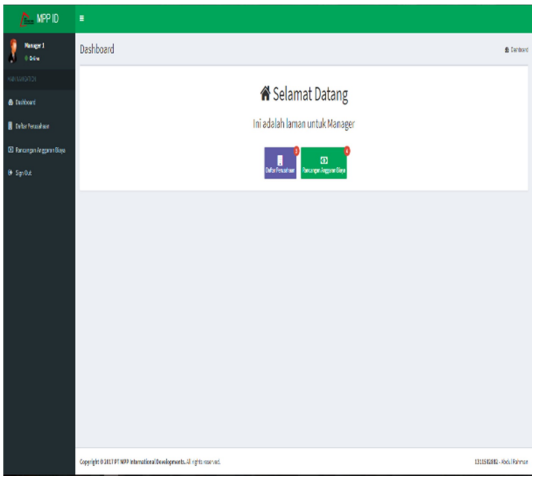
Tampilan layar *Dashboard* Sekretaris yang digunakan oleh sekretaris untuk mengisi data perusahaan dan rancangan anggaran biaya. Disini juga terdapat *menu Sign Out* apabila sekretaris ini keluar dari aplikasi. Bisa dilihat pada gambar berikut:



Gambar 4.4 : Tampilan Layar *Dashboard* Sekretaris

e. Tampilan Layar *Dashboard Manager*

Tampilan layar *Dashboard Manager* yang digunakan oleh sekretaris untuk mengisi data perusahaan dan rancangan anggaran biaya. Disini juga terdapat *menu Sign Out* apabila sekretaris ini keluar dari aplikasi. Bisa dilihat pada gambar berikut:



Gambar 4.5 : Tampilan Layar *Dashboard Manager*

5. PENUTUP

5.1 Kesimpulan

Dari tahap-tahap yang sudah dilakukan oleh developer dalam melakukan penelitian yang ada maka dapat disimpulkan beberapa kesimpulan yang ada sebagai berikut :

a. Dengan melakukan kombinisasi dalam menggabungkan dua algoritma yang ada ialah dengan algoritma Rivest Code 4 dan Lempel-Zev-Wei dalam mengamankan data yang ada pada PT. MPP International Development Indonesia supaya dapat lebih aman kerahasiaan dari orang-orang yang tidak bertanggung jawab.

b. Kecepatan penggunaan aplikasi sangat tergantung dengan *hardware* dan data yang akan dienkrip maupun didekrip.

c. Aplikasi yang dibuat ini yang dimana hanya dapat digunakan oleh user yang telah diijinkan atau diberi hak dalam mengakses aplikasi keamanan data yang telah dibuat.

5.2 Saran

Disini terdapat beberapa saran yang telah diterima penulis agar dapat membuat kemajuan atau pengembangan dalam aplikasi keamanan data yang telah dibuat.

a. *Interface* masih sangat sederhana diharapkan dapat dikembangkan beberapa fitur seperti *menu help, spam* dan lain sebagainya.

b. Dalam pengembangannya aplikasi ini dapat menggunakan lagi penambahan dalam algoritma lain sehingga dapat merangkap beberapa tipe data.

c. Dapat dikembangkan ke penelitian berikutnya untuk mempercepat proses enkripsi dan dekripsi data dokumen.

DAFTAR PUSTAKA

[1] Haji, W.H. et al., 2012. IMPLEMENTASI RC4 STREAM CIPHER UNTUK KEAMANAN BASIS DATA. , 2012(Snati), pp.15–16.

[2] Jumrin, Sutardi, S., 2016. Aplikasi sistem keamanan basis data dengan teknik kriptografi rc4. , 2(1), pp.59–64.

[3] Negara, L.S. & Kustian, N., 2014. SISTEM INFORMASI PENGAMANAN BASIS DATA. , 7(2), pp.188–199.

[4] Zarman, W., Pamungkar, T. & Hidayat, 2013. Teknik Komputer Unikom , Bandung Jurnal Ilmiah Komputer dan Informatika (KOMPUTA). , 2(1).

[5] Zebua, T., 2013. ANALISA DAN IMPLEMENTASI ALGORITMA TRIANGLE CHAIN Diterbitkan Oleh : STMIK Budi Darma

Medan Diterbitkan Oleh : STMIK Budi Darma
Medan. , III(April), pp.37–49.