METODE PENGAMANAN ENSKRIPSI RC4 STREAM CIPHER UNTUK APLIKASI PELAYANAN GANGGUAN

Asti Dwi Irfianti
Jurusan Teknik Informatika, Fakultas Teknologi Industri, UPN "Veteran" Jawa Timur
Gunung Anyar, Rungkut Surabaya
e-mail: asti@staffs.upnjatim.ac.id, asti_ilkom2000@yahoo.com

ABSTRAKSI

Aplikasi yang bersifat terpusat dan online 24 jam diperlukan agar dapat memonitoring keseluruhan kinerja dalam suatu instansi/perusahaan agar tidak perlu menunggu lama untuk mendapatkan respon informasi serta dapat diakses kapan pun ketika dibutuhkan.

Aplikasi web-base merupakan salah satu solusi untuk mewujudkan suatu aplikasi yang bersifat terpusat, akan tetapi karena aplikasi diakses dari media internet/intranet resiko data dicuri atau disalahgunakan oleh orang yang tidak bertanggung jawab pun semakin besar. Mengingat kebocoran data dapat disebabkan oleh orang dalam atau pihak-pihak yang berhubungan langsung dengan data.

Pengamanan data melalui metode enkripsi RC4 dapat menjadi salah satu solusi dalam hal pengamanan. Data yang ada tidak dapat langsung dibaca tanpa mengetahui secret key yang digunakan.

Kata kunci: *Data Security, Encryption, RC4 Stream Cipher*

1. PENDAHULUAN

Dalam penelitian ini penulis menggunakan studi kasus PT. PLN Distribusi Jawa Timur (PLN) sebagai perusahaan yang bergerak dalam bidang jasa ketenagalistrikan. PLN selalu berusaha memberikan pelayanan yang terbaik kepada para pelanggannya. Hal ini dapat diwujudkan bila perusahaan memiliki kinerja yang baik.

Berdasarkan pengamatan peneliti, dalam segi kecepatan, keakuratan dan keamanan dalam penyediaan informasi. selama ini ketika ada gangguan atau pemadaman terencana, Call Center atau operator gangguan di tiap area pelayanan mencatat pada suatu aplikasi lokal yang tidak terpusat, data jaringan mulai gardu induk sampai ke pelanggan masih tersimpan dalam bentuk kertas atau file biasa, dan belum adanya suatu aplikasi yang otomatis dapat menghitung kompensasi untuk pelanggan yang mengalami pemadaman melebihi standart yang ditetapkan oleh PLN.

Untuk itu peneliti memandang perlu untuk mengembangkan suatu aplikasi terpusat yang online 24 jam untuk mengetahui perkembangan gangguan dan pemeliharaan yang sedang terjadi, menyimpan data jaringan, selain itu dapat juga menghasilkan nilai kompensasi untuk pelanggan yang mengalami pemadaman melebihi standart yang ditetapkan PLN.

Karena sistem akan berjalan melalui media internet/intranet, oleh karena itu pengamanan terhadap data yang ada sudah menjadi persyaratan mutlak. Pengamanan terhadap jaringan komputer yang terhubung dengan data tidak menjamin keamanan data, karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak-pihak yang langsung berhubungan dengan data seperti administrator. Hal ini menyebabkan pengguna data harus menemukan cara untuk mengamankan data tanpa banyak campur tangan dari administrator data.

Dalam komunikasi data, terdapat suatu metode pengamanan data yang dikenal dengan Kriptografi (*Cryptography*). Menurut (Schneider, 1996) Kriptografi adalah seni dan ilmu untuk menjaga pesan rahasia agar tetap aman. Kriptografi adalah salah satu cabang ilmu algoritma matematika. Orang yang mempelajari dan menggemari kriptografi disebut *cryptographer*, sedangkan orang yang berusaha untuk memecahkan sandi kriptografi tersebut disebut *cryptanalyst*.

Dalam kriptografi terdapat berbagai macam sistem sandi (Cryptosystem) yang memiliki algoritma, tujuan penggunaan dan tingkat kerahasiaan berbeda. Dalam prakteknya, menentukan algoritma kriptografi yang digunakan menjadi suatu masalah tersendiri, di sisi lain user menginginkan kemudahan baik itu dari sisi kerahasiaan, ketepatan, kecepatan maupun biaya yang murah.

Kenyataan di lapangan, proses aplikasi dengan menggunakan metode kriptografi seringkali membutuhkan waktu yang relatif lebih lama dibandingkan tanpa proses kriptografi. Untuk itu perlu diciptakan suatu sistem sandi yang relatif cepat dalam proses penanganan data tanpa mengabaikan kaidah

kerahasiaan yang ingin dicapai, menurut (Brenton, 2005) sebuah sistem kriptografi tidak perlu menjadi tidak terpecahkan untuk menjadi berguna. Sistem hanya perlu dibuat cukup kuat untuk menahan serangan-serangan dari musuh selama informasi anda masih perlu dilindungi.

Peneliti memilih RC4 *stream cipher*, karena metode enkripsi dilakukan per karakter 1 byte untuk sekali operasi, jadi lebih hemat memory, RC4 merupakan salah satu cipher yang paling banyak digunakan di internet untuk pengaman SSL/TLS, dan RC4 menggunakan algoritma yang sederhana

dan mudah untuk diimplementasikan. (Kurniawan, 2004)

Harapan yang diharapakan dengan adanya aplikasi pelayanan gangguan dengan metode pengamanan enkripsi RC4 *stream cipher* adalah: 1) membuat aplikasi terpusat dan aman yang dapat menyediakan informasi mengenai gangguan, menyimpan data jaringan dan menghasilkan nilai kompensasi. 2) membuat suatu aplikasi yang dapat membantu pihak manajemen untuk mengontrol dan mengawasi kinerja pegawai dalam mengatasi gangguan. 3) menerapkan suatu metode kriptografi untuk mengamankan data yang ada.

2. METODE

2.1 Kriptografi, Enkripsi, dan Dekripsi

(Stiawan, 2005) Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*). *Crypto* berarti *secret* (rahasia) dan *graphy* berarti *writing* (tulisan).

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti (*Plaintext*) menjadi sebuah kode yang tidak bisa dimengerti (*Ciphertext*). Sedangkan proses kebalikannya untuk mengubah ciphertext mejadi plaintext disebut dekripsi. Sebuah sistem pengkodean menggunakan suatu table atau kamus yang telah didefinisikan untuk mengganti kata atau informasi atau yang merupakan bagian dari informasi yang dikirim. Secara umum operasi enkripsi dan dekripsi secara matematis dapat digambarkan sebagai berikut:

EK (M) = C {proses enkripsi}
DK (C) = M {proses dekripsi}

Pada proses enkripsi pesan M dengan suatu kunci K disandikan menjadi pesan C. pada proses dekripsi pesan C dengan kunci K disandikan menjadi pesan semula yaitu M. misalnya S (*sender*) mengirim sebuah pesan ke R (*receiver*) dengan media transmisi T. Di luar, ada O yang menginginkan pesan tersebut dan mencoba untuk mengakses secara ilegal pesan tersebut. O disebut *interceptor* atau *intruder*. Setelah S mengirim pesan ke R melalui media T, O bisa mengakses pesan tersebut dengan cara-cara sebagai berikut:

a. Menggangu pesan, dengan mencegah pesan sampai ke R.
b. Mencegat pesan, dengan cara mengetahui isi pesan tersebut.
c. Mengubah pesan dari bentuk aslinya dengan cara apapun.
d. Memalsukan pesan yang terlihat asli, jadi seolah-olah sebuah pesan dikirim oleh S.

Untuk melindungi pesan asli dari gangguan seperti ini dan menjamin keamanan dan kerahasiaan data maka mulai dikenal sistem kriptografi untuk melindungi data, yaitu dengan mengenkripsi pesan dan untuk bisa membaca pesan kembali seperti aslinya pesan harus didekripsi. Kriptografi merupakan cara yang paling praktis untuk melindungi data yang ditransmisikan melalui sarana telekomunikasi.

2.2 RC4 Stream Cipher

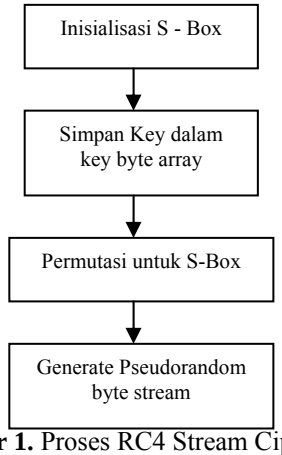
RC4 merupakan salah satu jenis *stream cipher* yang didesain oleh Ron Riverst di laboratorium RSA (RSA Data Security inc) pada tahun 1987. RC4 sendiri merupakan kepanjangan dari Ron Code atau Rivest's Cipher. RC4 *stream cipher* ini merupakan teknik enkripsi yang dapat dijalankan dengan panjang kunci yang variabel dan beroperasi dengan orientasi byte.

Algoritma yang sesungguhnya tidak dipatenkan oleh RSADSI, hanya saja tidak diperdagangkan secara bebas sampai sekarang. Namun pada bulan September 1994 ada seseorang yang telah mengirimkan sebuah *source code* yang diyakini sebagai RC4 ke *mailinglist* Cypherpunks dan keberadaannya pun langsung tersebar. Karena algoritma yang dipublikasikan ini sangat identik dengan implementasi RC4 pada produk resmi (Kurniawan, 2004)

2.3 Algoritma RC4 Stream Cipher

RC4 mempunyai sebuah S-box, $S_0,S_1,\ldots\ldots,S_{255}$, yang berisi permutasi dari bilangan 1 sampai 255. menggunakan dua buah indeks yaitu I dan J di dalam algoritmanya. Indeks I digunakan untuk memastikan bahwa suatu elemen berubah, sedangkan indeks J akan memastikan bahwa suatu elemen berubah secara random. Intinya, dalam algoritma enkripsi metode ini akan membangkitkan *pseudorandom byte* dari *key* yang akan dikenakan operasi Xor terhadap *plaintext* untuk menghasilkan *ciphertext*. Dan untuk menghasilkan *plaintext* semula, maka *ciphertext* nya akan dikenakan operasi Xor terhadap *pseudorandom byte*nya. Berikut ini akan diberikan sebuah bagan yang menggambarkan rangkaian proses yang dijalankan untuk mengenkripsi atau mendekripsi data.

Secara garis besar algoritma dari metode RC4 *stream cipher* ini terbagi menjadi dua bagian, yaitu: *key setup* dan *stream generation*.



Gambar 1. Proses RC4 Stream Cipher

Pada metode ini, proses enkripsi akan berjalan sama dengan proses dekripsinya sehingga hanya ada satu fungsi yang dijalankan untuk menjalankan kedua prose tersebut. Langkah-langkah yang akan ditempuh oleh program dalam menjalankan kedua proses tersebut meliputi hal-hal berikut ini:

a. User memasukkan *secret key* yang akan digunakan dalam proses enkripsi/dekripsi.
b. Lakukan proses inisialisasi awal S-Box berdasarkan indeksnya.
c. Simpan secret key yang telah dimasukkan user ke dalam array 256 byte secara berulang sampai array terisi penuh.
d. Bangkitkan nilai *pseudorandom* berdasarkan nilai key sequence.
e. Lakukan proses permutasi/transposisi nilai dalam S-Box selama 256 kali.
f. Bangkitkan nilai pseudorandom key byte stream berdasarkan indeks dan nilai S-Box.
g. Lakukan operasi XOR antara plaintext/ciphertext dan pseudorandom key byte stream untuk menghasilkan ciphertext/plaintext.

2.4 Mengatasi Masalah RC4

Untuk mengatasi permasalahan di atas, terdapat beberapa cara yang bisa dilakukan antara lain:

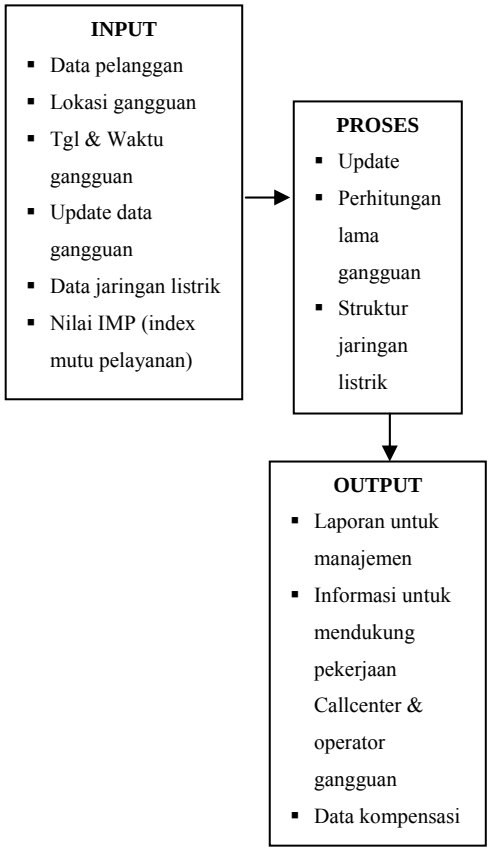
a) Gunakanalah kunci yang panjang (minimal panjang kunci ≥ 3 karakter dan maksimal ≤ 255 karakter) agar kemungkinan kunci dimasukkan berulang dalam key byte array semakin kecil dan gunakan kombinasi yang berlainan.
b) Usahakan untuk tidak menggunakan kunci yang sama untuk mengenkripsi file yang berbeda.
c) Jika kita akan menggunakan kunci yang sama untuk setiap kali mengenkripsi file, maka diperlukan *Initialization Vector* (IV) pada secret key. Jika IV yang digunakan untuk setiap kali proses enkripsi dijalankan tidak pernah sama maka akan dihasilkan ciphertext yang berbeda meskipun dienkrip plaintext yang sama.
d) Mengacak (mengubah susunan) plaintext sebelum diubah ke dalam cipher, sehingga jika seorang pengganggu memperoleh 1 byte data dari plaintext maka ia tidak dapat memperoleh data yang lainnya dengan cara meng-XOR-kan dua buah ciphertext dan byte data yang ia ketahui.
e) Mengubah metode pengisian key ke dalam key array. Caranya adalah key cukup diisikan sekali dalam array kemudian sisa variable array key yang lainnya akan diisi dengan nilai yang dibangkitkan secara random.

Berdasarkan keterangan di atas, dapat dilihat bahwa ada beberapa cara yang dapat digunakan sebagai solusi dari kekurangan yang terdapat dalam metode RC4 stream cipher.

2.5 Pelayanan Gangguan

Aplikasi ini awalnya mendapatkan inputan informasi gangguan dari pelanggan kepada CallCenter dan operator gangguan di area pelayanan\unit pelayanan jaringan atau informasi pemadaman terencana\perawatan dari operator gangguan di unit pelayanan distribusi. Selanjutnya sistem akan menyimpan data secara terpusat, diupdate jika gangguan telah diterima atau terselesaikan dan menghasilkan informasi untuk CallCenter, operator gangguan atau manajemen, sekaligus menghasilkan data nilai kompensasi kepada pelanggan yang berhak menerima. RC4 akan digunakan untuk mengamankan data user dan data nilai kompensasi sehingga data yang ada sulit untuk disalah gunakan oleh orang-orang yang tidak bertanggung jawab.

Aplikasi ini berjalan secara web-base, menggunakan jaringan WAN yang dimiliki oleh PLN, server web berada pada kantor distribusi PLN dan area pelayanan yang ada tinggal mengaksesnya menggunakan browser.

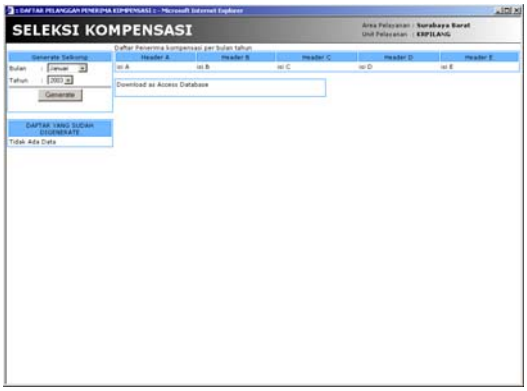


Gambar 2. Bagan aplikasi pelayanan gangguan

3. HASIL DAN PEMBAHASAN

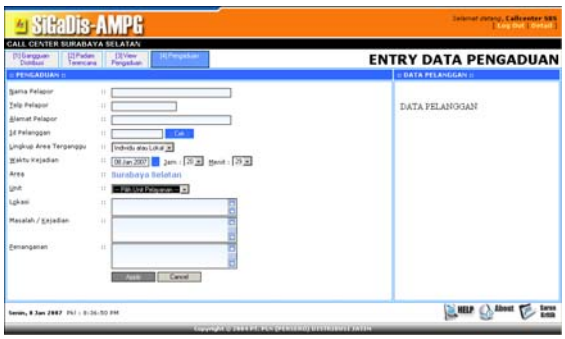
Pada tahap ini di uraikan hasil pengembangan aplikasi. Dari hasil survey dan wawancara dan diskusi pada saat penelitian di PLN didapatkan proses penanganan gangguan yang kemudian menjadi acuan dalam membangun aplikasi ini.

 ISSN: 1907-5022

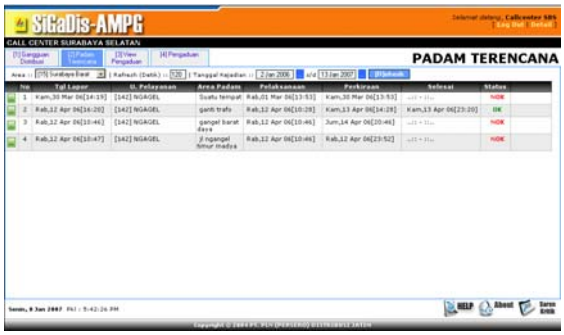


Gambar 3. Menu utama

Gambar 4. Entry Pengaduan



Gambar 5. View Padam Terencana



Gambar 6. Proses Selkomp

	idpel	kode_kompensasi
	160.35.37.190.114.13.197.240.141.202.247.49	164
	160.35.37.190.114.13.197.240.141.206.241.50	167
	160.35.37.190.114.13.197.240.141.206.243.55	161

Gambar 7. Hasil Selkom

PT PLN Distribusi Jawa Timur

Laporan Proses Seleksi Kompensasi
Periode Bulan Desember 2006

Area : Surabaya Barat
Jumlah : 5

Idpel	Kode
511010000351	1
511010000186	2
511010000152	1
511010000414	1
511010000489	1

Gambar 8. Laporan Selkomp

4. SIMPULAN

Beberapa kesimpulan yang didapatkan dari pembangunan aplikasi ini adalah: 1) Aplikasi ini memudahkan dalam proses menangani pengaduan, pemeliharaan, menyimpan data jaringan, menghasilkan nilai kompensasi dan laporan. 2) Penggunaan Secret Key yang panjang akan semakin baik untuk menciptakan keamanan yang lebih terjamin.3) Algoritma RC4 Stream cipher dapat digunakan sebagai salah satu teknik pengamanan data terhadap penyerangan dari pihak-pihak yang tidak bertanggung jawab.

PUSTAKA

Brenton, Christ. 2005. PT Elex Media Komputindo. *Network Security*. Jakarta

Berners-Lee, Tim. 2000. Texere. *Weaving the web: the past, present and future of the world wide web by its inventor*. San Francisco

Kurniawan,Yusuf. 2004. Informatika Bandung. *Kriptografi: Keamanan internet dan jaringan komunikasi.* Bandung

Kristanto, Andri. 2003. Gava Media. *Keamanan data pada jaringan komputer*. Yogyakarta.

Rahardjo, Budi. 1998-2005. PT Insan Infonesia – Bandung & PT INDOCISC – Jakarta, *Keamanan sistem informasi berbasis internet*, (Online), (http://www.ilmukomputer.org/2006/08/20/keamanan-sistem -informasi-berbasis-internet/, diakses 13 November 2006)

Stallings, William.1995. Prentice Hall. *Network and Internetwork Security*. NJ, USA.

Stiawan, Deris. 2005. PT Elex Media Komputindo. *Sistem keamanan komputer*. Jakarta

Schneier, B., John wiley & Sons, Inc.1996. *Applied Cryptography* (2rd ed). New York.

Sriwijaya Post. 2006, 26 maret. *Mengenal Teknik Kriptografi*. Hlm. 7.