KAJIAN ENKRIPSI DAN DEKRIPSI MENGGUNAKAN JARINGAN SYARAF TIRUAN DENGAN ALGORITMA PLATO

Anita Puspita Sari[1], Andrian Rakhmatsyah[2], Retno Novi Dayawati[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Enkripsi merupakan salah satu cara untuk menjaga atau melindungi data. Data yang telah dilakukan Enkripsi akan terjaga kerahasiaannya dimana orang lain tidak dapat membaca data tersebut. Isi dari data tersebut diubah sehingga tidak sesuai dengan data yang sebenarnya. Untuk dapat membaca kembali data tersebut maka dilakukan Dekripsi./br Pada tugas akhir ini telah diimplementasikan suatu sistem Enkripsi dan Dekripsi menggunakan jaringan Syaraf Tiruan menggunakan Algoritma Plato. Pelatihan pada JST plato dilakukan satu kali. oleh karena itu JST plato disebut sebagai algoritma sekali belajar. Data latih yang digunakan adalah berupa kata dimana trainer menentukan kata input dan kata target. Semua kemungkinan kata harus dilatihkan. Jika terdapat kata yang belum dilatihkan, maka hasil dekripsi tidak sesuai dengan file asli. Kata yang belum dilatih dikenali sebagai kata sebelumnya yang telah dilatihkan.
Waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi menggunakan algoritma plato dipengaruhi oleh jumlah kata. Semakin banyak jumlah kata yang digunakan maka semakin lama waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi. Sebaliknya semakin sedikit jumlah kata yang digunakan maka semakin cepat waktu yang dibutuhkan untuk enkripsi dan dekripsi. Waktu enkripsi dan dekripsi tersebut tidak dipengaruhi oleh kata yang belum dilatih, tanda baca, dan kata dalam bahasa asing.

Kata Kunci : Enkripsi, Dekripsi, Jaringan Syaraf Tiruan, Algoritma Plato.

Abstract

Encryption is one of method to keep or protect data. The secret of an encrypted data will be kept which the other people could not read that data. Content of data is changed so that there is no suitable content with truly data. To make data readable, we have to make a decryption method. This final assignment have been implemented an encryption and decryption system with Plato Artificial Neural Network. Encryption and decryption can be done by Plato Artificial Neural Network. The data trains one time in Plato Artificial Neural Network, so that Plato Artificial Neural Network is called one time training algorithm. The data train which used is words. The word must have input words and target words. All of word must be trained. If any untrained word is found, the result of decryption is not suitable to the original file. The untrained words are known as the trained former words.
Encryption and decryption time in the Plato algorithm is influenced by sum of words. The more sum of words have found in encryption and decryption process, the more time is needed to process. In contrary, the less sum of words have found, the less time is needed to process them. The encryption n decryption time is not influenced by untrained words, punctuation, and foreign words.

Keywords : Encryption, Decryption, Artificial Neural Network, Plato Algoritm

1. Pendahuluan

1.1. Latar belakang masalah

Keamanan merupakan hal yang sangat penting dalam menjaga serta melindungi aset atau data. Pada saat ini telah banyak berkembang sistem untuk mengamankan data. Keamanan data dapat dilakukan menggunakan steganografi atau kriptografi. Dalam hal ini penulis memfokuskan pengamanan data menggunakan kriptografi. Tujuan dari kriptografi itu sendiri adalah menjaga kerahasiaan, integritas, authentikasi serta non-repudiasi dari data. Metode yang terdapat pada kriptografi adalah Enkripsi dan dekripsi. Enkripsi merupakan metode untuk mengkodekan suatu data sehingga data tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Sedangkan Dekripsi adalah metode untuk menterjemahkan data yang telah dilakukan Enkripsi. Data yang akan dikirimkan akan diubah sedemikian sehingga orang lain tidak dapat mengenali isi data tersebut kecuali pemilik dari data tersebut[5].

Metode Enkripsi – Dekripsi sendiri sudah banyak berkembang dan penerapannya sudah banyak dilakukan oleh perusahaan. Terdapat Algoritma Enkripsi – Dekripsi yang telah dijamin kehandalannya dalam mengamankan data. Salah satu Algoritma Enkripsi – Dekripsi yang banyak digunakan adalah RSA[7]. Algoritma RSA merupakan algoritma yang memiliki tingkat kehandalan yang tinggi. Algoritma RSA merupakan algoritma yang sulit dibobol karena memiliki pemfaktoran yang amat rumit. Pada Algoritma RSA terdapat dua jenis kunci. Kunci tersebut adalah kunci publik dan kunci privat. Kunci publik merupakan kunci yang dipublikasikan. Sedangkan kunci privat merupakan kunci yang harus dijaga kerahasiaannya dari siapapun.

Jaringan syaraf tiruan adalah jaringan dari sekelompok unit pemroses kecil yang dimodelkan berdasarkan jaringan syaraf manusia. Jaringan syaraf tiruan merupakan sistem adaptif yang dapat merubah strukturnya untuk memecahkan masalah berdasarkan informasi eksternal maupun internal yang mengalir melalui jaringan tersebut. Jaringan Syaraf tiruan dapat digunakan untuk memodelkan hubungan yang komplek antara input dan output untuk menemukan pola-pola data. Jaringan syaraf tiruan sudah banyak dikembangkan serta diterapkan oleh berbagai bidang.

Pada Tugas Akhir ini, penulis mencoba mengenkrip data menggunakan Jaringan Syaraf Tiruan. Algoritma plato menggunakan neuron yang disederhanakan. Fungsi aktivasi yang digunakan algoritma Plato adalah fungsi step/*hardlimit*. Algoritma Plato memiliki tingkat kecepatan yang tinggi dibandingkan dengan algoritma lainnya. Salah satu contohnya adalah Algoritma Try-error. Keakuratan Algoritma Plato dapat dibuktikan dengan perhitungan. Algoritma Plato dapat mendefinisikan jumlah bit input dan bit output dalam jumlah yang besar tetapi masih memiliki nilai terhingga. Proses pelatihan dilakukan satu kali. Oleh karena itu algoritma Plato disebut sebagai algoritma ”sekali belajar”. Pelatihan pada enkripsi dan dekripsi memerlukan nilai bias dan bobot. Kelebihan algoritma plato adalah tidak semua data harus dilakukan

pelatihan. Algoritma plato dapat digunakan untuk melakukan enkripsi dan dekripsi pada text berita[1].

1.2. Perumusan masalah

Adapun perumusan masalah dalam Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana melakukan proses enkripsi – dekripsi menggunakan Jaringan Syaraf Tiruan dengan Algoritma Plato.
2. Bagaimana mengukur kecepatan dalam melakukan proses enkripsi – dekripsi menggunakan Jaringan Syaraf Tiruan dengan Algoritma Plato.
3. Bagaimana membandingkan Algoritma Plato dengan Algoritma RSA dalam melakukan enkripsi – deskripsi dengan Jaringan Syaraf Tiruan.

Untuk menjaga agar dalam penelitian tetap efektif, permasalahan tidak meluas, dan pembahasan tidak menyimpang dari tujuan serta menjadi mudah dipahami sesuai dengan tujuan penelitian yang hendak dilakukan, maka perlu dilakukannya pembatasan masalah sebagai berikut :

1. Proses enkripsi - dekripsi hanya dilakukan pada data berupa data (.txt).
2. Pada implementasi ini hanya melakukan proses enkripsi – dekripsi saja. Tidak menangani proses pengiriman hasil enkripsi dan penerimaan hasil deskripsi.
3. Pembangunan aplikasi menggunakan Matlab 7.0.1

1.3. Tujuan

Adapun tujuan yang hendak dicapai pada tugas akhir ini adalah sebagai berikut :

1. Mengimplementasikan Enkripsi dan Dekripsi menggunakan Jaringan Syaraf Tiruan dengan Algoritma Plato
2. Mengukur kecepatan proses enkripsi – dekripsi menggunakan jaringan syaraf tiruan
3. Melakukan perbandingan antara enkripsi – deskripsi menggunakan Jaringan Syaraf Tiruan dengan enkripsi – deskripsi menggunakan Algoritma RSA berdasarkan kecepatan pemrosesan. Membandingkan hasil enkripsi dan dekripsi dimana text dan spesifikasi *hardware* yang digunakan adalah sama.

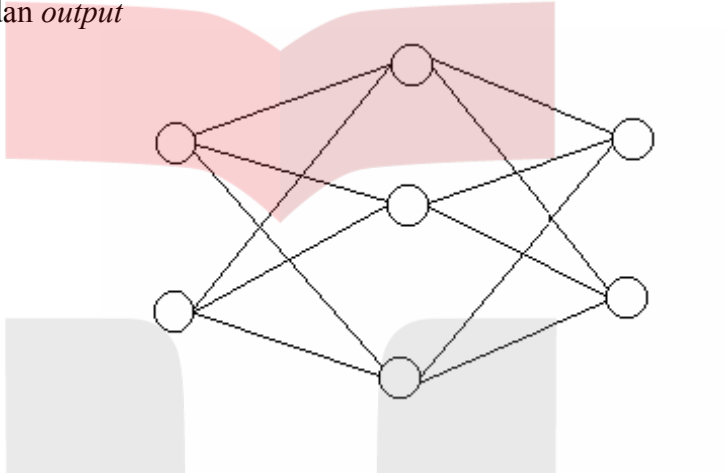
1.4. Metodologi penyelesaian masalah

Untuk menjawab berbagai permasalahan yang telah dirumuskan, berikut metodologi penyelesaian masalah yang dirumuskan :

1. Studi pustaka
   mendapatkan informasi dan referensi mengenai topik yang dibahas dari berbagai sumber seperti internet, buku dan pihak-pihak yang berkompeten di bidang ini.
2. Analisa Kebutuhan sistem
   - *Plaintext* yang digunakan untuk melakukan enkripsi – dekripsi
   - Arsitektur Plato untuk melakukan Jaringan Syaraf Tiruan

- Sistem pelatihan yang digunakan Plato

3. Perancangan sistem
   meliputi design dan cara kerja dari sistem, diantaranya adalah:
   - Plaintext akan diubah terlebih dahulu dalam bentuk biner. Hasil biner tersebut akan dilakukan proses enkripsi
   - Jaringan Syaraf Tiruan yang digunakan menggunakan 3 lapis yaitu *input*, tengah, dan *output*



Gambar 1-1 : Jaringan JST Plato

   - Menentukan jumlah bit *input* dan *output* untuk menghasilkan berapa node yang dapat dihasilkan pada layer tengah
   - Menentukan nilai *weight* dan bias semua node yang ada di lapis tengah
   - Setelah menentukan nilai *weight* dan bias maka akan dilakukan fungsi penjumlahan serta fungsi *treshold*.
   - Untuk melakukan proses dekripsi tersebut maka nilai biner hasi enkripsi akan dilakukan proses dekripsi.
4. Implementasi
   meliputi implementasi enkripsi serta dekripsi file text dengan Jaringan Syaraf Tiruan. Implementasi enkripsi dan deskripsi menggunakan Matlab 7.0.1.
5. Pengujian dan analisis
   melakukan pengumpulan data terkait dengan parameter yang telah didefinisikan. Menganalisa hasil implementasi dengan menggunakan parameter kecepatan dalam proses enkripsi – dekripsi menggunakan Jaringan Syaraf Tiruan dengan Algoritma Plato dibandingkan dengan enkripsi – dekripsi menggunakan Algoritma RSA.
6. Pembuatan laporan
   mendokumentasikan hasil perancangan, implementasi, dan analisa ke dalam sebuah laporan berbentuk *hardcopy* dan *softcopy*.

5. Kesimpulan dan Saran

Kesimpulan

Kesimpulan dari JST Plato adalah sebagai berikut:

1. Enkripsi dan dekripsi menggunakan algoritma Plato dapat dilakukan jika data yang digunakan telah dilakukan pelatihan.
2. Kata-kata yang belum dilatih, maka hasil dekripsi tidak sesuai dengan file atau data asli.
3. Jika pada saat pengujian terdapat kata-kata yang belum dilatih, maka kata tersebut dikenali sebagai kata sebelumnya dimana kata sebelumnya adalah kata yang telah dilatih. Jika kata-kata yang belum dilatih diletakkan di awal, maka tidak dapat dilakukan enkripsi .
4. Jika terdapat tanda baca pada kata-kata yang telah dilatih, maka kata tersebut dianggap berbeda dan dianggap sebagai kata baru. Oleh karena itu harus dilakukan pelatihan terlebih dahulu.
5. Waktu enkripsi dan dekripsi JST plato dipengaruhi oleh banyaknya kata yang diujikan. Adanya kata yang belum dilatih saat pengujian tidak mempengaruhi waktu enkripsi dan dekripsi.

5.2 Saran

Saran untuk menggunkan JST Plato dan untuk mengembangkan lebih lanjut:

1. Membuat mekanisme agar data belum dilatihkan dapat didekripsi sehingga hasil dekripsi dapat kembali ke plaintext asal.
2. Membuat mekanisme kunci yang cocok pada JST Plato. mekanisme kunci yang digunakan baik menggunakan asimetris (kunci enkripsi dan dekripsi sama) ataupun simetris (kunci enkripsi dan dekripsi berbeda) agar dapat menghasilkan nilai avalanche effect yang tinggi.
3. File yang diuji cobakan tidak hanya file text tetapi dapat berupa image, MP3, dll

Daftar Pustaka

[1] Iswadi, Aris, Harry, Prihanto, *Metoda Enkripsi – Dekripsi Menggunakan Jaringan Syaraf Tiruan Dengan Algoritma "Plato",* Jakarta : P3TB dan P3TFM BPPT, didownload pada tanggal 3 Desember 2007, waktu 11.45 WIB.

[2] Wikipedia, 2007, Jaringan saraf tiruan , http://id.wikipedia.org/wiki/Jaringan_saraf_tiruan, didownload pada tanggal 3 Desember 2007, waktu 13.20 WIB

[3] Jek Siang, Jong, *Jaringan Syaraf Tiruan dan Pemrograman Menggunakan Matlab,* Yogyakarta : ANDI, 2005.

[4] Abdia Away, Gunaidi, The Shortcut of MATLAB Programming, Bandung : INFORMATIKA, 2006.

[5] Enkripsi Data, http://students.ukdw.ac.id/~22033141/enkripsi.html, didownload pada tanggal 5 Desember 2007, waktu 15.12 WIB

[6] Aulia Adnan, Muhammad, *ASPEK HUKUM PROTOKOL PEMBAYARAN VISA/MASTERCARD SECURE ELECTRONIC TRANSACTION (SET)*, Jakarta: Fakultas Hukum Universitas Indonesia, 2000, didownload pada tanggal 4 Desember 2007 15.16 WIB

[7] Iqbal, Muhammad, *STUDI TEKNIS METODE ENKRIPSI RSA DALAM PERHITUNGANNYA*, Bandung : Institut Teknologi Bandung, didownload pada tanggal 5 Desember 2007, waktu 11.13 WIB

[8] *Measuring the Avalanche Effect of some Ciphers*, http://www.sfu.ca/~vkyrylov/JavaApplets/Cryptography.html, didownload pada tanggal 1 Juli 2008, waktu 10.28 WIB.

[9] *RSA Encryption and Decryption using Matlab*, http://www.mathwork/ECE575 Project - RSA Encryption & Decryption using Matlab.htm, didownload pada tanggal 4 Maret 15.19 WIB.

[10] Wikipedia, 2007, *Kriptografi*, http://id.wikipedia.org/wiki/Kriptografi, didownload pada tanggal 7 Juli 2007, waktu 11.19 WIB.

[11] An Introduction to Neural Network, http://www.cs.stir.ac.uk/~lss/NNIntro/InvSlides.html, didownload pada tanggal 5 Desember 2007, waktu 14.37 WIB

[12] Wikipedia, 2007, Enkripsi , http://id.wikipedia.org/wiki/Enkripsi, didownload pada tanggal 4 Desember 2007, waktu 10.19 WIB

[13] Pendahuluan, http://upi.yptk.ac.id/makalah/IDEA.pdf, didownload pada tanggal 5 Desember 2007, waktu 15.00 WIB

[14] Kriptografi, http://triadi.bagus.googlepages.com/Enkripsi-Dekripsi.pdf, didownload pada tanggal 6 Desember 2007, waktu 10.11 WIB

[15] Pengantar Jeringan Syaraf Tiruan, http://trirezqiriantoro.files.wordpress.com/2007/05/jaringan_syaraf_tiruan.pdf, didownload pada tanggal 10 Desember 2007, waktu 09.08 WIB

[16] Jaringan Syaraf Tiruan, http://inugzcakep.files.wordpress.com/2008/04/laporan-diskusi-dan-presentasi.pdf, didownload pada tanggal 10 Desember 2007, waktu 10.09 WIB