IMPLEMENTASI SECURE CHATTING (INSTAN MESSAGING) MENGGUNAKAN METODE ALGORITMA BLOWFISH BERBASIS WEB PADA PT. LAUTAN LEPAS NUSANTARA

Camelia Nurani[1)], Siswanto[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1.2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : camelia24@gmail.com[1)], siswanto@budiluhur.ac.id[2)]

ABSTRAK

Perusahaan PT. Lautan Lepas Nusantara membutuhkan pengamanan dalam hal pengunaan *chatting*. Aplikasi pengiriman pesan instan (*Instan Messaging*) sudah menjadi hal umum untuk digunakan dan mendukung kemudahaan komunikasi. PT. Lautan Lepas Nusantara yang bergerak dibidang perdaganggan dan import melakukan komunikasi terhadap *customer* dan *supplier* melalui layanan *InstantMessanging* yang bisa digunakan oleh karyawan adalah *Email dan Whatsapp*, namun aplikasi ini melakukan enkapulasi terhadap pesan berupa *plaintext* (tidak menggunakan metode enkripsi) sehingga seseorang *attacker* dapat membaca pesan yang dikirim dengan mudah. Maka dari itu dibuatlah system *Secure Chatting (Instan Messanging)* menggunakan aplikasi enkripsi dan deskripsi dengan menggunakan Algoritma *Blowfish* merupakan algoritma modern kunci simetris berbentuk *cipher* blok yang melakukan peroses enkripsi dan deskripsi pada teks yang dikirim dengan kombinasi kunci yang hanya diketahui oleh pengguna. Hasil dari pengujian yang di dapatkan bahwa untuk enkripsi dan dekripsi pesan atau karakter tidak membutuhkan banyak waktu hanya tidak melebihi 1 detik. Kesimpulan yang di dapat jumlah karakter hampir tidak mempengaruhi waktu proses enkripsi dan dekripsi.

Kata Kunci : *Secure Chatting, Instant Messaging*, Algoritma *Blowfish*, *Prototype*, Php

1. PENDAHULUAN

PT. Lautan Lepas Nusantara (LLN) merupakan perusahaan yang bergerak di bidang perdagangan dan importer mesin, peralatan dan perlengkapan petanian perlengkapan elektronik dan telekomunikasi dan bagian-bagian lainnya., merek enternity, infinity dan lainnya, PT. Lautan Lepas Nusantara juga merupakan distributor hampir di seluruh provinsi Indonesia, mulai dari Palembang, Lampung, Pekan baru, Jambi, Surabaya. PT. Lautan Lepas Nusantara menggunakan media Telepon dan Internet untuk melakukan kegiatan transaksi, promosi, serta komunikasi kepada semua coustemer dan konsumen. *Internet* telah mengubah cara berkomunikasi dan berbisnis. Salah satu cara berkomunikasi menggunakan internet yaitu dengan menggunakan layanan *e-mail*. Untuk itu diperlukan aplikasi *Instant Messenger(IM)* yang dapat berkomunikasi secara*real-time*. Pada umumnya *Instan Messenger* lebih praktis digunakan karena *user* hanya perlu memilih *user*. Selain itu untuk memenuhi keperluan komunikasi berbasis *Instant Messenger (IM)* tidak memerlukan penggunaan memori yang besar. Karena aplikasi yang dibuat sebenarnya berbasis web namun dibuat sedemikian rupa agar dapat digunakan dalam bentuk aplikasi android. Serta, aplikasi ini dibuat untuk keamanan rahasia pada sebuah pesan agar tidak mudah dibaca oleh pihak yang tidak berkepentingan.

Pertukaran informasi yang terjadi dapat bersifat sensitif dan dikelola dengan sistem yang tidak aman. Informasi yang bersifat sensitif tersebut dapat berupa informasi perusahan/bisnis atau bahkan informasi pribadi. Sangat mudah bagi seseorang untuk melakukan pihak korban, menghilangkan kepercayaan pelanggan dan membuat perselisihan.

Beragam cara untuk menanggulangi *eavesdropping* atau *modification*, diantaranya yaitu dengan enkripsi, dimana dalam penelitian ini menggunakan algoritma enkripsi *Blowfish*. Algoritma enkirpsi *Blowfish* digunakan karena algoritma ini dianggap sangat aman, dapat diandalkan, belum dapat dibongkar oleh *cryptoanalyst* manapun sampai saat ini karena tidak mempunyai kelemahan yang berarti (Ibrahim, 2012).

Maksud dari penelitian ini adalah untuk merancang aplikasi *instant messenger (chatting)* yang aman. Dengan adanya beberapa permasalahan yang ada,
dan dapat mempermudah perusahaan yang membutuhkan keamanaan data, yang sangat fatal jika

ada kebocoran kerahasiaan data pada perusahaan tersebut, dan dapat mengakibatkan kebangrutan ada manipulasi pesan asli.

2. LANDASAN TEORI

2.1 Kriptografi

Kriptografi berasal dari bahasa yunani, dan terdiri dari dua suku kata uyang berarti kripto dan graphia. Keriptografi artinya menyembunyikan dan graphia artinya adalah tulisan. Kriptografi adalah ilmu yang mempelajari tentang teknik-teknik ilmu matematika yang berhubungan dengan aspek keamanann informasi, seperti keabsahan data perusahaan, auntentikasi data perusahaan, kerahasiaan data perusahaan, namun dari banyak masalah terhadap keamaanan data tidak semua dapat diselesaikan oleh kriptografi.. kriptografi banyak pula yang mengatakan bahwa kriptografi sebagai ilmu seni yang berguna untuk keamanan data perusahaan.

Kriptografi memiliki 4 komponen utama yaitu:

a. Plaintext, adalah pesan yang masih berbentuk pesan asli dean masih dapat di baca dengan jelas.
b. Chipertext, adalah pesan yang sudah di rubah dan sehingga tidak dapat dibaca lagi .
c. Key, adalah kunci untuk membuka pesan yang tidak dapat di baca atau pesan untuk membuka kriptografi itu sendiri.
d. Algoritma, adalah metode yang digunakan untuk melakukan enkripsi dan deskripsi.

Di dalam keilmuan kriptografi meliputi 2 proses dasar adalah: (Pabokory, Astuti, & Kridalaksana, 2015):

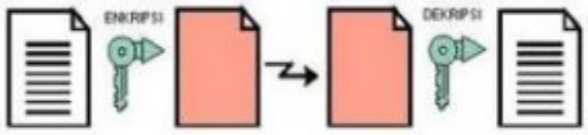
a. Enkripsi (*Encryption)*
b. Deskripsi (*Decryption*).

Dan tujuan kriptografi adalah:

a.Kerasahasiaan : wadah yang digunakan untuk menjaga kerasiaan data yang telah ada dan hanya dapat dilihat oleh pihak tertentu yang sudah memiliki kunci rahasia yang digunakan untuk membuka ataupun untuk menghapus datang yang sudah dikunci.
b.Non-repudiasi adalah untuk dapat mencegah terjadinya penyangkalan terhadap pengirim atau terciptanya suatu informasi oleh yang telah mengirim atau yang telah membuat.
c. Integrasi data adalah yang berhubungan sdengan pengenalan ataupun identifikasi, yang untuk menjaga data secara tidak sah, yang digunakan mengidentifikasi seseotrang yang telah memanipulasi data oleh pihak yang tidak berhak. Yaitu, penyisipan, penghapusaan, dan pensubtitusian data lain kepada data yang sebenarnya.
d. Authentifikasi adalah pengenalan baik secara kesatuan maupun informasi untuk sendiri. Yang sebelum dikirim harus melalui pengecekan keasliannya dari isi datanya,waktu pengirim dan lain-lainnya.

a. Algoritma Kriptografi Simetris

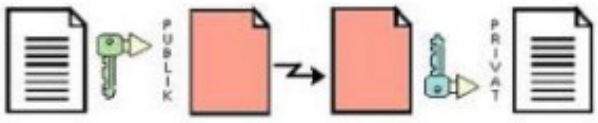
Algoritma kriptografi konvensional dapat disebut algoritma simetris. Algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Algoritma Asimetri dapat dibagi menjadi dua ketegori yaitu algoritma blok (Blok Chipers) dan algoritma aliran (Stream Chiper). Algoritma blok proses penyediaannya akan berorientasi pada sesekumpulan bit data, sedangkan algoritma aliran berorientasi haya pada satu bit data. Contoh algoritma asimetris adalah DES (Data Encryption Standard), Blowfish, Twofish, MARS, IDEA, 3DES (DES dapat diaplikasikan 3 kali), AES(Asvanced Encryption Standard) yang bernama asli Rijndael.



Gambar 1. Kunci Simetris(Basri, 2016).

b. Algoritma Kriptografi Asimetri

Algoritma Asimetri adalah algoritma yang menggunakan kunci yang berbeda untuk melalukan proses enkripsi dan deskripsi. Kunci enkripsi dapat disebarkan secara umum dan dapat disebut kunci public (public key) dan sedangkan kunci deskripsi disimpan untuk diunakan untuk pribadi sendiri dan dapat dinamakan sebagai kunci pribadi (private key) maka dari itu kunci ini dikenal sebagai kunci public (public key cryptography) contoh algoritma yang dikenal sebagai kunci algoritma asimetris adalah .RSA (Riverst Shamir Adleman) dan ECC (Elliptic Curve Crypthography). Terdapat dua kunci yaitu kunci publik dan kunci pribadi, kunci public didistibusikan untuk umum dan kunci pribadi di distribusikan untuk sendiri.



Gambar 2. Penggunaan Kunci Simetris (Basri, 2016).

2.2Algoritma *Blowfish*

Algoritma blowfish merupakan algoritma blok cipher 64 bit/byte dengan panjang kunci variable.algoritma ini dibagi menjadi 2 bagian yaitu : *key expansion* atau peluasan kunci dan enkripsi pada data. *Expansion* dapat merubah kunci mencapai 448 bit/byte menjadi beberapa array sub kunci dengan total 4168 bit/byte. Enkripsi data terdapat dari iterasi fungsi sederhana.

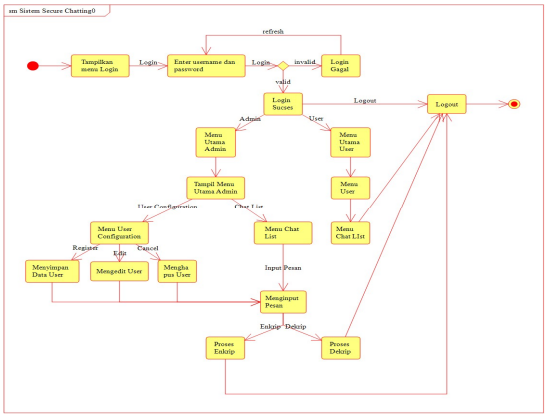
(Wardoyo, Imanullah, & Fahrizal, 2016).

3.ANALISA DAN PERANCANGAN PROGRAM

3.1 Skema Proses Aplikasi

Aplikasi ini dibuat oleh penulis, dan pada Penelitian ini adalah aplikasi yang telah dibuat berbasis *website*, yang telah dikembangkan oleh bahasa pemrograman *php*. Berikut adalah langkah-langkah proses aplikasi :

a. *User* menginput username dan *password* untuk bisa masuk ke halaman utama sebuah aplikasi, disini dapat 2 yang dapat login yaitu user dan admin
b. *User* login sebagai admin dan user nika login sebagai admin maka akan muncul menu untuk configuration
c. Setelah menginput username dan password *user* akan diarahkan ke halaman utama aplikasi. Dimana admin dapat memulai percakapan dengan *user* lain yang ada pada halaman tersebut dengan cara mengklik salah satu *user*. Selain itu, admin juga dapat melakukan *user configuration*.
d. Maka user dapat mengechat user lainnya dengan memilih caht list yang sudah ada.
e. Setelah *user* menginput pesan yang akan di kirim maka sertver akan mengenkripsi secara otomatis.
f. Untuk proses deskripsinya di dalam tampilan chatlist akan muncul *messagebox* untuk mengiput *password*.
g. Kemudian *user* akan melihat hasil deskripsi.



Gambar 3.:State Diagram Proses Keseluruhan Aplikasi

3.2 Perangkat Yang Digunakan

Perangak keras yang dibutuhkan dalam membangun perangkat lunak ini memiliki spesifikasi:

a. Perangkat Keras (*Hardware*)

Perangkat keras komputer yang digunakan dalam pengembangan sistem ini terdiri dari satu buah laptop Axioo dengan spesifikasi sebagai berikut :

1) CPU : Intel® Core™ i5
2) Hardisk : 400 GB.
3) RAM : 2.00 GB.
4) Monitor : 14.0"
5) Keyboard : Internal Keyboard Laptop.

b. Perangkat Lunak (*Software*)

Perangkat lunak yang digunakan untuk menunjang kelancaran dalam pembuatan aplikasi ini memiliki spesifikasi:

1) Sistem Operasi : Windows 8
2) *Tools Editor* : Sublime Text 3Java
3) *Local Server* : XAMPP v1.8.3, PHP v5.5.15

3.3 Spesifikasi Basis Data

a. Tabel Data Keseluruhan *User*

Berikut adalah database pada user, atribut di bawah akan menjelaskan keseluruhan database user :

Tabel 1 : Atribut Data Keseluruhan User

Field	Type	Length	Keterangan
id_user	Int	11	*id user*
username	Varchar	20	nama masuk
password	Varchar	100	kata sandi
nama	Varchar	50	nama pengguna
level	Int	1	*Level User*

b. Tabel Data Keseluruhan *Chat*

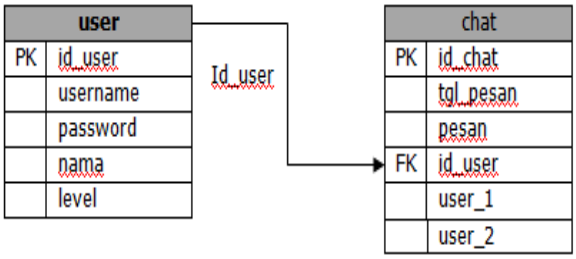
Berikut adalah database pada user, atribut di bawah akan menjelaskan keseluruhan database user :

Tabel 2 : Atribut Data Keseluruhan Chat

Field	Type	Length	Keterangan
id_chat	Int	10	*Auto_increment*
user_1	int	11	User 1
user_2	int	11	User 2
Created_at	timestamp	10	Tanggal pesan
pesan	text	100	Isi pesan

c. LRS (Logical Record Struktur)

Bentuk dari ERD (*Entity Relationship Diagram*) yang ditransformasikan menjadi LRS (*Logicanl Record Structured*)

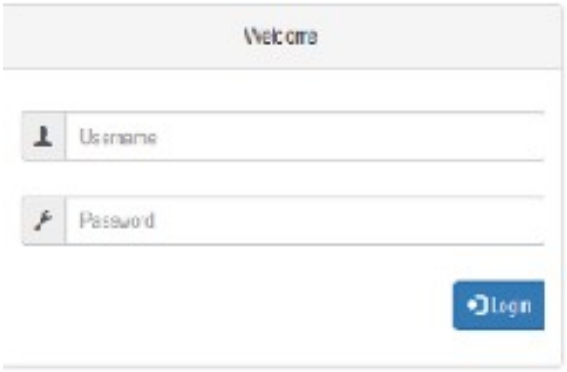


Gambar 4.LRS (Logical Record Struktur)

4. implementasi dan uji coba program

a. Tampilan Form Layar Utama

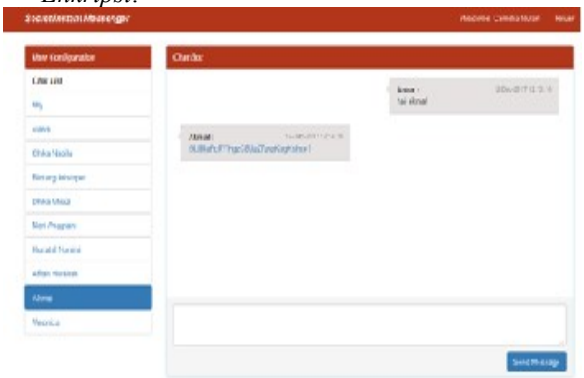
Menu utama adalah tampilan layar yang ditampilkan pertama kali kepada *user*. Tampilan layar ini terdapat beberapa menu yaitu ada menu login, menu utama admin, menu utama user, *configuration*.



Gambar 5. Tampilan Form Layar Utama

b. Tampilan Form Layar *Enkripsi*

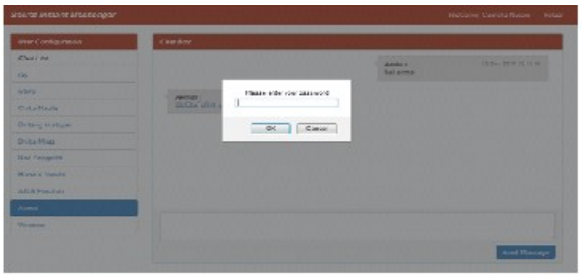
Menu form *enkripsi* ini akan muncul jika user sedang mengirim pesan kepada user lain. *Enkripsi*.



Gambar 6. Tampilan Form enkripsi

c. Tampilan Layar Form Deskripsi

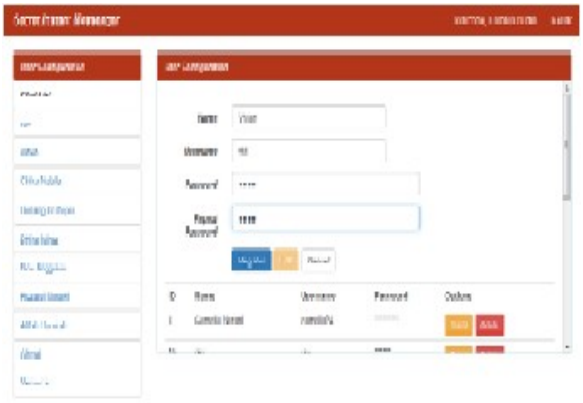
Menu form Deskripsi ini akan muncul *Messagebox* untuk menginput *password*.



Gambar 7. Tampilan Form Deskripsi

d. Tampilan Form Layar Configuration

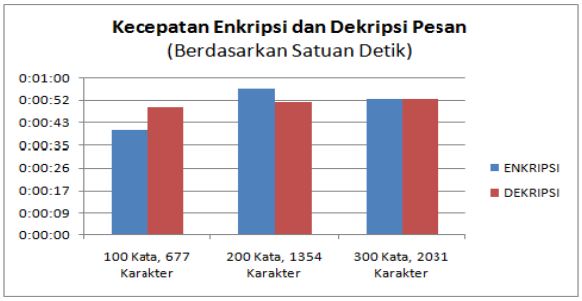
Menu form Configuration ini akan muncul jika admin ingin menginput user baru dan mendelet, edit uuser yang sudah ada.



Gambar 8. Tampilan Form Configuration

e. Tampilan Grafik Hasil Uji Coba

Pada tabel grafik ini dapat dilihat hasil kecepatan enkripsi dan deskripsi pesan teks bedasarkan satuan karakter,sanngat tidak memerlukan waktu yang lama, bahkan tidak lebih dari 1 detik untuk melakukan enkripsi dan deskripsi pada penelitian ini.



Gambar 9.Tampilan Grafik Hasil Uji Coba

5. PENUTUP

5.1 Kesimpulan

Setelah seluruh hasil Penelitian ini selesai, maka disimpulkan bahwa menggunakan algoritma *Blowfish* berbasis website dan dapat mempermudah PT. Lautan Lepas Nusantara mempermudah dalam

berkomunikasi kepada konsumen, Dengan mengimplementasikan algoritma *Blowfish*, pesan yang tersimpan dalam database merupakan pesan berbentuk *ciphertext.* Serta ditampilkan pada jendela *Chat Box* dalam bentuk *ciphertext.* Sehingga dipastikan terhindar dari serangan *eavesdropping,* Jumlah karakter sangat tidak mempengaruhi waktu proses enkripsi dan dekripsi.

5.2 Saran

Berdasarkan beberapa kesimpulan di atas, maka penulis dapat memberikan saran berupa :

Pada penelitian selanjutnya diharapkan dapat menambahkan fitur lain selain karakter teks. Misalnya, gambar berekstensi .jpg, .jpeg, .png, .swf, dokumen berekstensi .doc, .docx, .xls, .xlsx, .pdf, video berekstensi .mp4, .flv, dan sebagainya.

Daftar pustaka

[1] Basri. (2016). KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM PERSPEKTIF KEAMANAN DATA DAN KOMPLEKSITAS KOMPUTASI. *Jurnal Ilmiah Ilmu Komputer*, *2*(2), 17–23.

[2]Handoko, P., & Kom, M. (2016). KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITMA VIGENERE CIPHER DAN STEGANOGRAFI DENGAN METODE END OF FILE (EOF) TEKNIK, 1–7.

[3]Ibrahim, R. N. (2012). Kriptografi Algoritma Des, Aes/Rijndael, Blowfish Untuk Keamanan Citra Digital Dengan Menggunakan Metode Discrete Wavelet Transformation (Dwt). *Jurnal Computech & Bisnis*, *6*(2), 82 – 95.

[4]Wardoyo, S., Imanullah, Z., & Fahrizal, R. (2016). Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android. *Jurnal Nasional Teknik Elektro*, *5*(1), 37–44.

[5]Widodo, R. (2014). Penerapan Kriptografi Blowfish dan One Time Pad (OTP) untuk Keamanan Data pada PT. Bangun Indah Permai. *Perpustakaan Universitas Budi Luhur*, *5*.