BAB I
PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi *chatting* semakin banyak yang digunakan oleh masyarakat. Perkembangan seperti ini mengubah dunia menjadi sangat efisiensi tentunya waktu dan biaya. Bahkan fasilitas *chatting* seakan menjadi kebutuhan sehari-hari bagi penggunanya hampir semua teknologi memberikan fasilitas *chatting* karena dengan kemudahannya manusia untuk berkomunikasi saling bertukar informasi.

Instant Messenger atau lebih dikenal dengan IM hadir dengan beberapa fitur yang telah umum disediakan diantaranya :

a. *Chat*

   Dapat melakukan percakapan dengan kontak baik berupa teks maupun berupa suara atau video.

b. *Buddy list & Online Information*

   Menyimpan daftar kontak yang telah didaftarkan teman serta mengetahui siapa saja dari kontak teman tersebut yang sedang *online* atau tersedia untuk melakukan percakapan.

c. *Conference*

   Selain dapat melakukan percakapan yang bersifat privat, juga dapat melakukan percakapan dengan orang banyak apabila masuk kedalam *chat room* tersebut.

d. *File Transfer*

   Memungkinkan untuk dapat berkirim file dengan teman.

Karena beberapa fitur diatas, *instant messenger* merupakan aplikasi yang paling banyak digunakan saat ini. Tercatat pengguna aplikasi *instant messenger Windows Live* mencapai 10 juta pengguna di Asia Tenggara. Angka tersebut belum ditambah dengan aplikasi IM lainnya telah banyak dipakai.

Dari data tersebut mencerminkan bahwa penggunaan teknologi informasi cukup pesat. Seiring dengan berkembangnya penggunaan *instant messeger* maka

aspek keamanan menjadi salah satu hal yang sangat penting. Terutama untuk pesan yang bersifat *private* yang memungkinkan orang lain tidak bisa membacanya.

Symantec Enterprice Security (2006:7) menyatakan bahwa, *instant messeger* rentan terhadap serangan :

a. *Eavesdropping*

   Mengingat kebanykan instant messenger tidak mengenkripsi lalu lintas jaringan maka pihak ketiga berpotensi besar untuk menguping pembicaraan yang sedang dilakukan dan umumnya menggunakan sebuah paket *sniffer* dan teknologi yang sejenis.

b. *Account Hijacking*

   Kebanyakan sistem *instant messeger* rentan terhadap pembajakan akun dan penyamaran. Sebagaimana yang dialami oleh Butet Kertaradjasa seorang pelawak dan pemain teater yang kehilangan uang Rp.2,5 Juta karena akun YM nya dibajak oleh orang yang tidak bertanggung jawab.

c. *Data Access and Modification*

   Seperti kebanyakan perangkat lunak yang terhubung ke internet, bisa memiliki *bug* yang dapat menjadi celah penyerang untuk dapat mengakses data dan memodifikasinya.

d. *Worm and Blended Threats*

   Platform instant messenger juga memungkinkan untuk dapat penyebar *worm* dan ancaman lainnya yang juga berbahaya.

Berdasarkan hasil analisis dari symantec Enterprise Security, *eavesdropping* atau lebih dikenal dengan penyadapan menempati urutan pertama dalam kasus penyerangan terhadap *instant messeger*. Hal ini terjadi karena *instant messenger* yang banyak digunakan tidak mengenkripsi pesan yang dikirim sehingga memudahkan pihak ketiga untuk membaca pesan tersebut.

Arie Karhendana (2006:14) melakukan pengujian keamanan paket data yang ditransmisikan selama proses komunikasi berlangsung terhadap program *instant messenger* yang populer saat ini YM dan *Windows Live Messeger*. Hasil pengujian tersebut menunjukan bahwa layanan *Yahoo Messenger* dan *Windows Live* sama sekali tidak aman karena data dapat dengan mudah disadap.

Untuk mencegahnya dapat digunakan menggunakan ilmu kriptografi WAKE *(Word Auto Key Encryption)* termasuk kedalam algoritma simetris. Penyimpanan kunci jelas sangat penting untuk pengamanan sistem enkripsi secara menyeluruh. Kunci yang disimpan secara tidak baik akan mudah untuk dicuri oleh pihak yang tidak diinginkan. Solusi untuk penyimpanan kunci beraneka ragam, mulai dari penggunaan hardware khusus dimana semua proses kriptografi dilakukan didalam *hardware* khusus dan kunci enkripsi disimpan dan tidak dapat keluar dari *hardware*, sampai dengan penyimpanan dalam file yang dienkripsi menggunakan *password*. Karena praktis, metode terakhir sangat populer, yang berarti pengamanan *password* menjadi penting. Dengan demikian data yang dikirim tidak mudah untuk dibaca oleh *attacker.*

I.2 Perumusan Masalah

Bagaimana merancang dan membangun aplikasi *chatting* berbasis *client-server* dengan enkripsi algoritma kriptografi WAKE.

Untuk menjawab rumusan masalah diatas, muncul beberapa pertanyaan:

a. Bagaimana membuat aplikasi *chatting client-server*?
b. Bagaimana menambahkan enkripsi menggunakan algoritma WAKE?

I.3 Ruang Lingkup Penelitian

Ada beberapa ruang lingkup penelitian pada tugas akhir ini, antara lain:

a. Membuat aplikasi *chatting* untuk komunikasi *Client-Server*.
b. Aplikasi ini berjalan platfom Windows

I.4 Tujuan Penelitian

Bagi penulis tujuannya untuk memberikan kemudahan komunikasi aplikasi *chatting* yang dilengkapi dengan pengaturan hak akses *Client.*

Bagi masyarakat ilmiyah hasil penelitian ini diharapkan menambah wawasan dalam hal penyimpanan data.

I.5 Manfaat Penelitian

Salah satu manfaat penelitian ini adalah meningkatkan keamanan informasi dalam menyimpan data secara metode WAKE. Karena seorang penyerang bisa melihat komunikasi data yang berlangsung pada saat *chatting.*

I.6 Sistematika Penulisan

Sistematika penulisan penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, Perumusan Masalah, Ruang Lingkup Penelitian, tujuan Penelitian, Manfaat Penelitian dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Bab ini berisi pembahasan mengenai berbagai macam konsep dasar dan teori yang menunjang dan ada kaitannya dengan topik tugas akhir yang diambil. Seperti: Aplikasi, algoritma, dan *tools* yang digunakan dalam membuat tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai perancangan dari aplikasi yang akan didasarkan pada teori.

BAB IV PERANCANGAN DAN IMPLEMENTASI

Bab ini menjelaskan mengenai rancangan umum aplikasi, implementasi algoritma WAKE *(word auto key encryption)* pada aplikasi *chatting*, dan pengujian aplikasi yang telah dibuat.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan penutup, yang di dalamnya berisi kesimpulan dari seluruh rangkaian penelitian serta saran yang diharapkan dapat bermanfaat untuk pengembangan pembuatan sistem.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN