	KEMENTRIAN PENDIDIKAN DAN KEBUDAYAAN UNIVERSITAS BRAWIJAYA FAKULTAS TEKNIK JURUSAN TEKNIK ELEKTRO Jalan MT Haryono 167 Telp & Faks. 0341 554166 Malang 65145	**KODE** **PJ-01**

PENGESAHAN
PUBLIKASI HASIL PENELITIAN SKRIPSI
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK UNIVERSITAS BRAWIJAYA

NAMA : BAYU ADITYA HERLAMBANG

NIM : 105060300111041- 63

PROGRAM STUDI : REKAYASA KOMPUTER

JUDUL SKRIPSI : IMPLEMENTAS PELOMPATAN IP DALAM BAHASA C

Telah diperiksa dan disetujui oleh :

Pembimbing 1	Pembimbing 2
Dr. Ir. Muhammad Aswin, M.T.	**Raden Arief Setyawan, S.T., M.T.**
NIP: 19640626 199002 1 001	**NIP: 19750819 199903 1 001**

IMPLEMENTAS PELOMPATAN IP DALAM BAHASA C

PUBLIKASI JURNAL SKRIPSI

Diajukan Untuk Memenuhi Sebagian Persyaratan

Memperoleh Gelar Sarjana Teknik

DISUSUN OLEH :

BAYU ADITYA HERLAMBANG

NIM. 105060300111041-63

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS BRAWIJAYA

MALANG

2015

Implementasi Pelompatan IP dalam Bahasa C

Bayu Aditya Herlambang[1], Ir. Muhammad Aswin, M.T.[2], Raden Arief Setyawan, S.T., M.T.
Teknik Elektro Universitas Brawijaya
[1]b@yuah.web.id, [2]maswin@ub.ac.id, [3]rarief@ub.ac.id

Abstract — Information security is the practice of de-fending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction, in order to provide integrity, confidentiality, and reliability of information. In fact, each data transmission between computers has the potential loss of one or more characteristics of the information security. In data transmission, each data packet has the same identity that the IP address that can be used by intruders as the merging data stream reference and data can be obtained even if the whole data has been encrypted.

The main objective of this research is to build a system that capable of sending a series of data which the destination IP address/port is switch rapidly, using predetermined pseudorandom sequence to improve confidentiality of data transmission.

The assessments confirm the advantages of IP hopping in improving the confidentiality of data transmission between computers as compared to other protocol marked by with a correlation coefficient of -0,00014 compared with FTP at 0 (zero). IP hopping maximum transfer speed is 295,76 KiB/seconds or 4,85 percent of FTP transfer speed.

***Index Terms**: Socket, IP Address, Port, IP hooping.*

Abstraksi — Keamanan informasi memiliki makna melakukan pelindungan informasi dan sistem informasi dari akses tanpa wewenang, penggunaan, penyingkapan, gangguan, pengubahan, atau penghancuran, dalam rangka menyediakan keutuhan, kerahasiaan, dan kehandalan. Dalam kenyataannya, dalam setiap pengiriman data antar komputer memiliki potensi kehilangan satu atau lebih karakteristik keamanan informasi tersebut. Dalam pengiriman data, setiap paket data memiliki identitas yang sama yakni alamat IP yang dapat digunakan oleh penyusup sebagai acuan penggabungan aliran data. Dengan menggunakan acuan itu, data utuh dapat diperoleh walaupun data tersebut telah terenkripsi.

Penelitian ini memiliki tujuan untuk membangun sistem yang mampu melakukan transfer data antar komputer dengan melakukan pengubahan alamat IP/porta tujuan pengiriman secara cepat berdasarkan acak semu yang ditentukan.

Hasil pengujian yang telah dilakukan menjelaskan pelompatan IP memiliki kelebihan dalam meningkatkan kerahasiaan pengiriman data antar komputer dibandingkan dengan protokol lain yang ditandai dengan nilai koefisien korelasi sebesar -0,00014, lebih tinggi dibandingkan dengan protokol FTP yang memiliki nilai sebesar 0 (nol). Pelompatan IP memiliki kecepatan maksimal 295,76 KiB/detik atau 4,85 persen dari kecepatan protokol FTP.

Kata kunci: Soket, Alamat IP, Porta, Pelompatan IP.

I. PENDAHULUAN

Keamanan informasi memiliki makna melakukan pelindungan informasi dan sistem informasi dari akses tanpa wewenang (*unauthorized access*), penggunaan, penyingkapan, gangguan, pengubahan, atau penghancuran, dalam rangka menyediakan keutuhan, kerahasiaan, dan kehandalan (44 U.S. Code § 3542) [1].

Dalam kenyataannya, dalam setiap pengiriman data antar komputer memiliki potensi kehilangan satu atau lebih karakteristik keamanan informasi tersebut. Misalnya dalam pengiriman suatu data antar komputer dalam suatu jaringan komunikasi yang melalui banyak sambungan (*nodes*), memiliki potensi penyusupan yang dilakukan oleh pihak ketiga di salah satu sambungan tersebut. Pihak ketiga tersebut dapat mengetahui data yang dikirimkan antara pihak pertama, yakni pihak yang pertama kali melakukan atau meminta pengiriman, dan pihak kedua, yakni pihak kedua, yakni pihak yang menerima kiriman atau melakukan pengiriman atas permintaan pihak pertama.

Selain dapat melakukan pembacaan data yang ditransmisikan tersebut, pihak ketiga juga dapat melakukan manipulasi/pengubahan data yang menyebabkan sifat dan/atau isi dari data tersebut berubah. Atau pihak ketiga tersebut melakukan peniruan pihak kedua sehingga pihak pertama menganggap bahwa pihak ketiga adalah pihak kedua sehingga melakukan pengiriman data kepada ketiga.

Enkripsi digunakan untuk melindungi data dalam transmisi dengan cara melakukan pengacakan dengan pola tertentu yang hanya diketahui oleh pengacak, dalam hal ini pengirim, dan oleh pengurai, dalam hal ini penerima. Pihak ketiga yang tidak berhak seharusnya tidak dapat mengetahui pola tersebut dan menggunakannya untuk menguaikan informasi yang diperoleh.

Untuk menemukan pola enkripsi, penyusup dapat melakukan uji statistik dari aliran transmisi yang diperolehnya dengan cara mencari keteraturan dalam ketidakteraturan aliran tersebut. Semakin besar keteraturan dalam aliran tersebut, semakin besar kemungkinan penyusup mengetahui pola dari enkripsi tersebut sehingga dapat diuraikan dengan semakin cepat.

Metode pengiriman data yang umum digunakan saat ini adalah metode pengiriman di mana seluruh data dikirim ke tujuan dengan pengenal yang sama, yakni alamat IP. Alamat IP adalah bagian dari Protokol Internet (*Internet Protocol).*

Internet Protocol (IP) merupakan protokol yang memiliki tugas mengirim paket data dari komputer sumber ke komputer tujuan berdasarkan alamat IP dan pengepala (*headers*) paket (Cerf , V.: 1974)[2]. Dalam melakukan pengirimannya, IP menerima pecahan data, yang disebut paket data, dari *Transmission Control Protocol* (TCP), yaitu protokol yang digunakan untuk menyediakan layanan komunikasi antara program aplikasi dan IP, yang menyebabkan ukuran data yang dikirimkan dalam satu waktu menjadi semakin kecil.

Namun, dalam setiap paket tersebut memiliki identitas yang sama yakni alamat IP yang dapat digunakan oleh penyusup sebagai acuan penggabungan aliran data. Dengan menggunakan acuan itu, data utuh dapat diperoleh walaupun data tersebut telah terenkripsi.

Pelompatan IP (*IP hooping*) merupakan metode yang digunakan untuk menyembunyikan urutan paket tersebut. Dalam metode pelompatan IP, setiap paket data yang dikirimkan memiliki alamat IP tujuan yang terus berubah setiap waktu selama pengiriman data. Alamat IP yang berubah bisa berbeda komputer atau satu komputer yang sama.

II. TINJAUAN PUSTAKA

A. Soket Jaringan

Soket secara umum digunakan untuk interaksi klien dan peladen. Pengaturan umum yang digunakan menggunakan peladen di satu komputer dengan klien di komputer lainnya. Klien menghubungi peladen, bertukar informasi, dan lalu memutuskan sambungan (IBM Knowledge Center)[3].

Sebuah soket memiliki aliran kejadian yang umum. Dalam model klien ke peladen berorientasi sambungan, soket dalam proses peladen menunggu permintaan dari klien. Untuk melaksanakan ini, peladen harus mengikat (*binds*) suatu alamat yang klien bisa lakukan permintaan layanan. Pertukaran data klien-peladen terjadi bila klien menyambung ke peladen melalui soket, Peladen melaksanakan permintaan klien dan mengirim balasan ke klien.

B. RSA

RSA merupakan salah satu teknik implementasi kriptografi publik-privat pertama yang secara luas digunakan untuk transmisi data aman. Kunci enkripsi yang digunakan adalah bersifat publik dan berbeda dengan kunci deskripsi yang disimpan.

RSA menggunakan kunci publik dan kunci privat. Kunci publik bisa dimiliki oleh siapa saja dan digunakan untuk menyandikan pesan dan hanya dapat dipecahkan oleh kunci privat (Rivest: 1978)[4]. Kunci untuk algoritma RSA dibuat dengan cara berikut:

1. Pilih dua angka prima yang berbeda, *p* dan *q*. Untuk keamanan, nilai bulat yang dipilih *p* dan *q* harus dipilih secara acak dan panjang bit harus sama.
2. Hitung *n=p*q*. *n* digunakan untuk modulus untuk kunci privat dan publik. Panjang n, biasanya dalam bit, merupakan panjang kunci.
3. Hitung $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, dengan φ adalah Fungsi Phi Euler.
4. Pilih bilangan bulat e dengan $1 < e < \varphi(n)$ dan $FPB(e,\varphi(n))=1$; *FPB* adalah Faktor Persekutuan terbesar; *e* dan $\varphi(n)$ adalah koprima, yakni FPB kedua bilangan adalah 1. *e* sebagai eksponen kunci publik; *e* memiliki panjang bit pendek dan hasil Bobot Hamming (Hamming Weight) di enkripsi yang lebih efisien, umumnya 216 + 1 = 65.537. Namun, nilai yang lebih kecil e (misalnya 3) diketahui kurang aman di beberapa pengaturan.
5. Tentukan d sebagai $d \equiv e-1 \pmod{\varphi(n)}$; d adalah pengalian inversi modular dari *e(modulo φ(n))*. Lebih jelas ditentukan bila *d* adalah $d \cdot e \equiv 1 \pmod{\varphi(n)}$. *d* disimpan sebagai eksponen kunci privat.

Bila ingin melaksanakan penyandian/enkripsi, kunci publik (*e* dan *n*) diberikan oleh penerima kepada pengirim.

Dalam enkripsi, pengirim mengubah pesan *M* ke bilangan bulat *m*, dengan $0 \le m < n$.

Lalu menghitung *cipher text c*, yakni:

$$c \equiv m^{e} \pmod{n}$$

Dalam dekripsi, penerima mengembalikan m dari c menggunakan kunci privatnya dan eksponen d dengan

$$m \equiv c^{d} \pmod{n}$$

menghasilkan m lalu mengubah kembali pesan ke M dengan cara yang terbalik.

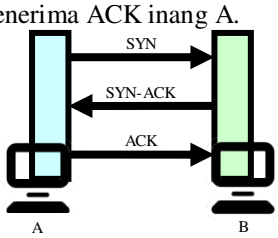
C. Salt

Salt, secara harfiah adalah garam, merupakan kata atau karakter tambahan yang digunakan untuk menambah panjang sumber masukan untuk cincangan (*hash*) yang dihasilkan dari fungsi pencincang (*hash function*), yakni fungsi yang berfungsi membuat data sama panjang (*fixed-length output data*) yang memiliki kaitan dengan data sumber (Ullrich: 2011)[5].

D. Jabat Tangan TCP

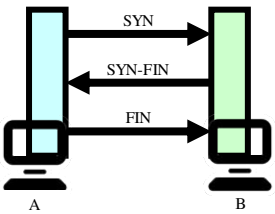
Dalam komunikasi antar perangkat, TCP menggunakan tiga langkah jabat tangan untuk membangun sambungan (RFC 793)[6]. Langkah membangun sambungan adalah sebagai berikut:

1. Inang pengirim (A) mengirim paket sinkronisasi (SYN) ke penerima (B).
2. Inang B menerima paket SYN inang A.
3. Inang B mengirim pengakuan sinkronisasi (SYN-ACK) ke inang A.
4. Inang A menerima SYN-ACK inang B.
5. Inang A mengirim ACK.
6. Inang B menerima ACK inang A.



Gambar 1. Membuka sambungan TCP.

Setelah sambungan terjalin, pengiriman data dilakukan. Sinkronisasi (SYN) dan pengakuan (ACK) ditentukan oleh bit yang terdapat dalam pengepala TCP. Bila sambungan antar perangkat berhenti, tiga langkah jabat tangan juga dilakukan untuk melepaskan sambungan. Paket yang kirim dalam memutus sambungan adalah paket FIN sebagai pengganti ACK.



Gambar 2. Menghentikan sambungan TCP.

E. Korelasi Diri

Korelasi Diri (*Auto Correlation*) dapat digunakan untuk dua kegunaan sebagai berikut:

1. Mendeteksi ketidakacakan dalam data.
2. Mengenali model rangkaian waktu yang tepat bila data tidak acak (Filliben)[7].

Korelasi Diri dapat dihitung, misal dengan nilai Y_1, Y_2, ...Y_N, dalam waktu X_1, X_2, ...X_N dan jeda k sehingga memiliki rumus:

$$r_k = \frac{\sum_{i=1}^{N-k} (Y_i - \overline{Y})(Y_{i+k} - \overline{Y})}{\sum_{i=1}^{N} (Y_i - \overline{Y})^2}$$

Dengan X adalah variabel waktu dan Y adalah nilai uji. Walaupun variabel waktu, X, tidak digunakan dalam formula ini, dianggap bahwa ruang waktu yang digunakan sama.

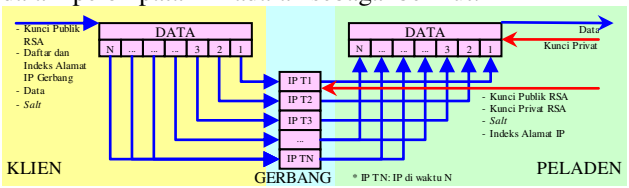
Korelasi Diri adalah koefisien korelasi/pertalian. Namun, bukan pertalian yang terjadi antara dua variabel yang berbeda, tapi hubungan antara dua nilai dari variabel yang sama pada waktu X_i dan X_{i+k}.

Semakin hasil mendekati nilai 0 (nol), maka memiliki pertalian yang terjalin semakin tinggi. Semakin mendekati 1 (satu), pertalian yang dimiliki semakin rendah. Pertalian yang terjalin ini menandakan ketidakacakan data. Semakin tinggi korelasi data, maka semakin rendah keacakan data tersebut.

III. DESAIN DAN IMPLEMENTASI

A. Abstraksi Sistem

Sistem komputasi pengiriman dan penerimaan data dalam pelompatan IP adalah sebagai berikut:

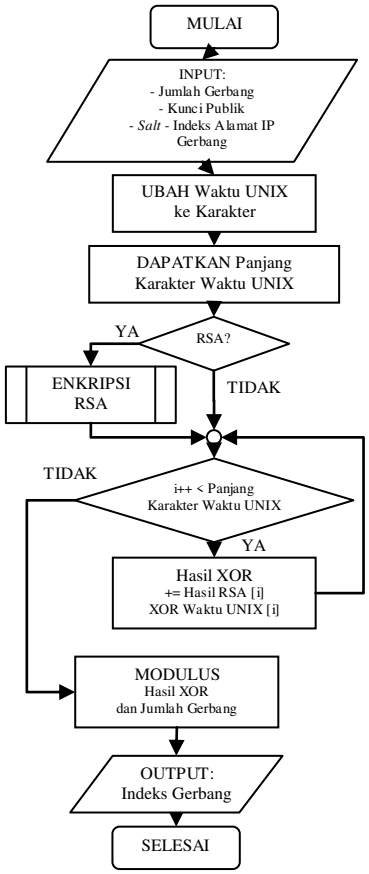


Gambar 3. Abstraksi Sistem.

Langkah kerja:

1. Program untuk klien, gerbang, dan peladen telah diatur memiliki publik RSA dan *salt* dan klien memiliki daftar alamat-alamat IP peladen yang digunakan.
2. Pengguna memberi masukan berupa argumen program yang berisi data yang akan dikirimkan dalam sintaks bahasa C yang sahih, yakni berupa berkas atau karakter yang dikirimkan.
3. Program klien memecah data tersebut menjadi paket-paket sebesar sesuai yang telah, lalu diantrekan untuk menunggu dikirimkan.
4. Program klien, gerbang, dan peladen melakukan pengacakan berdasarkan kunci publik peladen, selanjutnya paket antrean pertama dienkripsi menggunakan teknik RSA dan dikirim menuju alamat IP gerbang yang dipilih berdasarkan hasil pengacakan yang telah ditentukan.
5. Program gerbang menerima dari klien, bila alamat gerbang tidak sesuai, maka paket ditolak oleh program gebang. Paket yang sahih dilanjutkan ke program peladen.
6. Program Peladen menerima data telah dikirim oleh program klien melalui program gerbang lalu dideskripsi RSA menggunakan kunci privat peladen kemudian menyusunnya berdasarkan urutan alamat IP dan data yang sesuai dengan hasil pengacakan yang telah dilakukan oleh Program Peladen.

B. Pemilihan IP

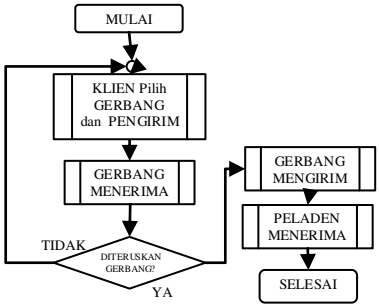


Gambar 4. Bagan Alur Pemilihan IP.

Langkah pemilihan IP adalah

1. Mengubah angka Waktu UNIX menjadi karakter huruf Waktu UNIX; lalu
2. mendapatkan panjang karakter Waktu UNIX; lalu
3. hasil enkripsi RSA dari kunci publik dengan masukan berupa *salt* yang telah ditentukan, bila menggunakan enkripsi; lalu
4. diambil karakter sebanyak panjang Waktu UNIX; lalu
5. setiap karakter Waktu UNIX dan hasil enkripsi RSA diubah ke angka; lalu
6. dilakukan penjumlahan operasi XOR setiap karakter hasil enkripsi RSA dan karakter Waktu UNIX; lalu
7. dilakukan operasi modulus jumlah Gerbang; kemudian
8. hasil adalah alamat IP terpilih.

C. Pelompatan IP



Gambar 5. Bagan Alur Pelompatan IP.

Langkah pelompatan IP adalah sebagai berikut:

1. Klien memilih Gerbang sesuai dengan pemilihan alamat IP.

2. Gerbang menolak atau meneruskan ke Peladen berdasarkan pemilihan alamat IP. Bila indeks alamat IP yang dipilih sesuai dengan identifikasi Gerbang maka meneruskan ke Peladen.
3. Bila ditolak oleh Gerbang, Klien mengulangi langkah nomor 1. Bila tidak ditolak, Gerbang meneruskan ke Peladen.
4. Peladen menerima data.
5. Program Klien diakhiri, Gerbang dan Peladen bersiaga.

D. Spesifikasi Pecahan

Pecahan merupakan pecahan yang dikirim setiap transfer data. Berikut ini adalah spesifikasi pecahan:

Of-set	Ok-tat	0	1	2	3
Ok-tat	Bit	00 01 02 03 04 05 06 07	08 09 00 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
0	0	Pengepala			
4 … 1024	32 … 8192	DATA			

Gambar 6. Spesifikasi Pecahan.

a. Protokol TCP.
b. Panjang pecahan sebesar 1024 bita (8192 bit); yakni
   i. 4 bita (32 bit) pengepala; dan
   ii. 1020 bita (8160 bit) data.

E. Spesifikasi Pengepala

Pengepala merupakan bita awal dari pecahan yang berisi identifikasi unik dari pecahan. Berikut ini adalah spesifikasi pengepala:

Of-set	Ok-tat	0	1	2	3
Ok-tat	Bit	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
0	0	Versi (00 01 02) / Panji (03 04) / Paritas (05) / SG (06) / SP (07)	Identifikasi Pecahan		Identifikasi Data

Gambar 7. Spesifikasi Pengepala.

a. **Versi**. Versi yang digunakan. Untuk laporan ini menggunakan versi 1. Sehingga memiliki nilai biner 001.
b. **Panji**/Flag
   i. 01: START, paket pecahan awal;
   ii. 11: IN-TRANSFER, paket pecahan tengah kirim;
   iii. 10: STOP, paket pecahan akhir; dan
   iv. 00: INVALID, paket pecahan diabaikan.
c. **Paritas**. Bit-paritas digunakan hanya untuk memeriksa keutuhan data. Bit-paritas yang digunakan adalah bit-paritas genap.
d. **SG**. Status Gerbang. Status penerimaan oleh Gerbang. 1 adalah berhasil dan 0 adalah gagal.
e. **SP**. Status Peladen. Status penerimaan oleh Peladen. 1 adalah berhasil dan 0 adalah gagal.
f. **Identifikasi Pecahan**. Nomor urut paket pecahan yang dikirim.
g. **Identifikasi Data**. Identifikasi data. Digunakan agar bila ukuran data melebihi ukuran Identifikasi Pecahan, data dapat digabungkan dengan benar.

F. Spesifikasi Pecahan Awal

Pecahan awal merupakan pecahan yang dikirimkan oleh Klien kepada Peladen dengan isi data berupa informasi mengenai berkas yang dikirimkan. Pecahan awal ditandai dengan pengiriman panji START. Pecahan awal selalu dikirimkan sebagai pecahan dengan identifikasi 0 (nol).

Setiap bagian dibatasi oleh karakter Carriage Return-Line Feed (CRLF, ASCII indeks 13 dan 10). Selain itu juga menggunakan karakter titik (DOT, ASCII indeks 46) sebagai pemisah angka desimal di waktu.

```
Isi data pecahan awal:
Identifikasi berkas [CRLF]
ukuran berkas [CRLF]
nama berkas [CRLF]
```

Keseluruhan merupakan data jenis *string*.

G. Spesifikasi Pecahan Akhir

Pecahan akhir merupakan pecahan yang dikirimkan oleh Klien kepada Peladen dengan sebagai penanda bahwa rangkaian pengiriman telah berakhir. Pecahan akhir ditandai dengan panji STOP. Pecahan akhir memiliki identifikasi di bawah jumlah maksimal pecahan atau jumlah maksimal pecahan.

Bila pecahan akhir telah diterima Peladen, Peladen dapat melakukan tindakan penulisan berkas dari tembolok memori ke diska.

Isi bidang data adalah kosong. Seluruh bidang data di panji akhir memiliki nilai NULL (ASCII indeks 0 (Nol)).

H. Spesifikasi Balasan Peladen

Selain pengepala, Peladen juga memberikan balasan di bidang data. Setiap bagian dibatasi oleh karakter Carriage Return-Line Feed (CRLF, ASCII indeks 13 dan 10). Selain itu juga menggunakan karakter titik (DOT, ASCII indeks 46) sebagai pemisah angka desimal di waktu.

Balasan peladen berguna sebagai umpan balik kepada Klien sehingga mengetahui perkembangan pengiriman sehingga dapat Klien dapat memberikan tindakan yang sesuai, misal menghentikan pengiriman atau mengetahui perbedaan waktu Klien dan Peladen.

Balasan Peladen berupa:

```
Identifikasi Berkas [CRLF]
Ukuran Berkas [CRLF]
Ukuran Diterima [CRLF]
Waktu Unix Detik [DOT]
Waktu Unix Mikrodetik [CRLF]
```

Keseluruhan merupakan data jenis string.

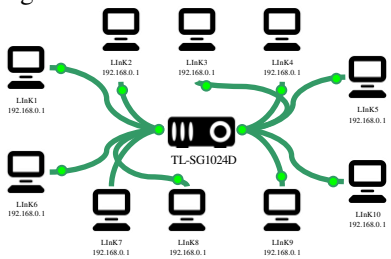
Isi balasan peladen dimulai dari bita awal pecahan hingga maksimal ukuran maksimal pecahan. Bita sisa dari pecahan yang tidak digunakan oleh Balasan Peladen diberikan nilai NULL (ASCII indeks 0 (Nol)).

I. Konfigurasi Perangkat Keras

Perangkat keras yang digunakan terdiri atas:

- 10 unit komputer personal: Intel Dual Core E5400, DDR2 2GB.
- *switch* TL-SG1024D dan pengabelan UTP Cat 5e

Konfigurasi jaringan lokal menggunakan topologi bintang, sebagai berikut:



Gambar 8. Topologi Jaringan.

J. Konfigurasi Perangkat Lunak

Perangkat lunak yang digunakan:

1. GNU/Linux kernel 3.13.0-46-generic mesin 32 bit dan 64 bit;
2. glibc 2.19, gcc 4.8.2;
3. OpenSSL 1.0.1f

IV. PENGUJIAN

Pengujian menggunakan berkas teks polos dengan ukuran tiap pengiriman sebesar 1 (satu) MiB (angka basis 2 (2^{10} bita)) dengan jumlah pengiriman sesuai dengan jenis pengujian. Kecuali disebutkan lain, jumlah Gerbang adalah sejumlah 8 (delapan) dengan 1 (satu) Peladen dan 1 (satu) Klien.

A. Protokol Pembanding

Protokol pembanding yang digunakan adalah *File Transfer Protocol* (FTP).

Dilakukan pengujian dengan melakukan serangkaian pengiriman berkas sebanyak 200 kali dan dilakukan perhitungan rata-rata untuk kecepatan dan tingkat keberhasilan pengiriman berkas.

Ke-	Berhasil	Waktu (detik)	Kec. (B/d)
1.	YA	0,303940	3.449.944,07
2.	YA	0,154028	6.807.697,30
3.	YA	0,169764	6.176.668,79
4.	YA	0,163145	6.427.264,09
5.	YA	0,158410	6.619.380,09
6.	YA	0,164332	6.380.838,79
7.	YA	0,156976	6.679.849,15
8.	YA	0,158212	6.627.664,15
9.	YA	0,161934	6.475.329,46
10.	YA	0,303940	3.449.944,07

Tabel 1. Sampel Percobaan Transfer FTP.

Didapati nilai untuk kecepatan adalah 6.244.794,89 B/detik (5,95 MiB/detik) dan nilai untuk keberhasilan 100 persen. Selain itu juga dilakukan perhitungan nilai keacakan dari pilihan tujuan pengiriman menggunakan rumus Korelasi Diri.

Detik ke-	Indeks tujuan	Koefisien Korelasi
1.	0	1,00000000000000000
2.	0	0,00000000000000000
3.	0	0,00000000000000000
4.	0	0,00000000000000000
5.	0	0,00000000000000000
56.	0	0,00000000000000000
57.	0	0,00000000000000000
58.	0	0,00000000000000000
59.	0	0,00000000000000000
60.	**0**	**0,00000000000000000**

Tabel 2. Sampel Percobaan Transfer FTP.

Didapatkan nilai 0 (nol) sebagai tanda bahwa nilai tersebut memiliki relasi yang tinggi, sehingga nilai tersebut memiliki keacakan yang rendah.

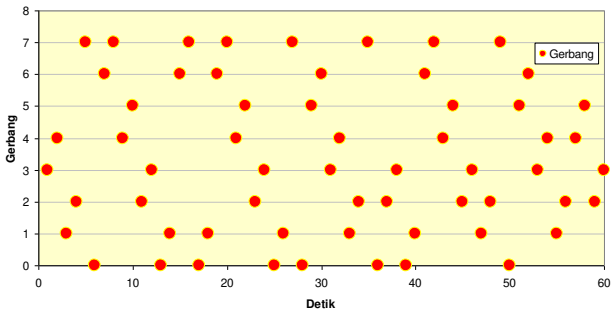
B. Penyebaran Gerbang

Percobaan dengan cara melakukan pengiriman selama 60 detik ke sejumlah 8 (delapan) Gerbang.

Detik ke-	Indeks Gerbang	Koefisien Korelasi
1.	3	1,00000000000000000
2.	4	-0,03184480220079420
3.	1	-0,03187295794487000
4.	2	0,04080312699079510
5.	7	-0,04688354954123490
56.	2	0,00059961673105136
57.	4	-0,00057594064855948
58.	5	0,00029903007089160
59.	2	0,00049226527335122
60.	**3**	**-0,00014092570927460**

Tabel 3. Sampel Pengiriman ke Gerbang.

Berikut ini bagan pengiriman ke Gerbang.



Gambar 9. Bagan Penyebaran Gerbang tiap Detik.

Tampak bahwa dalam tiap detik, Gerbang yang dipilih adalah merata dan acak semu yang sesuai dengan spesifikasi Pemilihan IP (butir 4.1.3 halaman 24) dan memiliki nilai koefisien korelasi sebesar -0,00014, lebih tinggi daripada FTP sebesar 0 (nol). Hal ini sebagai penanda bahwa pecahan data yang dikirimkan memiliki keacakan yang lebih tinggi, sehingga Pelompatan IP memiliki tingkat kerahasiaan yang lebih baik.

C. Jumlah Sambungan

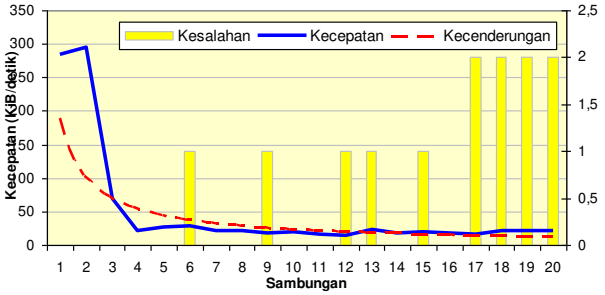
Percobaan ini dilakukan untuk mengetahui hubungan antara jumlah sambungan pengiriman dengan rata-rata kecepatan dan persen tingkat keberhasilan serta perbandingan kecepatan protokol pembanding.

Dilakukan pengujian dengan melakukan serangkaian pengiriman sebanyak 200 kali dan dilakukan perhitungan rata-rata untuk kecepatan dan tingkat keberhasilan pengiriman berkas.

Samb.	Berhasil	Persen Berhasil	Kec. (B/d)	Persen Kec. FTP
1.	200/200	100,0%	291.665,91	4,67
2.	200/200	100,0%	302.862,50	4,85
3.	200/200	100,0%	71.618,19	1,15
4.	200/200	100,0%	22.535,42	0,36
5.	200/200	100,0%	26.563,27	0,43
6.	199/200	99,5%	28.661,42	0,46
7.	200/200	100,0%	21.304,56	0,34
8.	200/200	100,0%	21.744,84	0,35
9.	199/200	99,5%	19.031,18	0,30
10.	200/200	100,0%	20.172,69	0,32
11.	200/200	100,0%	16.170,36	0,26
12.	199/200	99,5%	14.771,36	0,24
13.	199/200	99,5%	23.284,44	0,37
14.	200/200	100,0%	17.816,85	0,29
15.	199/200	99,5%	19.482,66	0,31
16.	200/200	100,0%	18.128,61	0,29
17.	198/200	99,0%	16.949,92	0,27
18.	199/200	99,0%	21.002,78	0,34
19.	198/200	99,0%	21.020,76	0,34
20.	198/200	99,0%	22.482,53	0,36

Tabel 4. Transfer Paralel.

Berikut ini adalah bagan tiap sambungan.



Gambar 10. Bagan Pembanding antara Kecepatan dan jumlah Sambungan.

Tampak bahwa 2 (dua) sambungan memiliki kecepatan yang paling tinggi dibandingkan sambungan tunggal dan sambungan paralel lain. Selain itu, terdapat potensi kesalahan pengiriman semakin tinggi sebanding dengan jumlah sambungan.

D. Pengiriman Terenkripsi

Percobaan ini dilakukan untuk mengetahui perbandingan antara sambungan terenkripsi dan tak terenkripsi.

Dilakukan pengiriman sebanyak 50 kali dan dilakukan perhitungan rata-rata untuk kecepatan dan tingkat keberhasilan pengiriman berkas.

Lalu dilakukan pembandingan antara jumlah sambungan pengiriman dengan rata-rata kecepatan dan persen tingkat keberhasilan serta perbandingan kecepatan dengan sambungan yang tidak terenkripsi.

Ke-	Berhasil	Waktu (detik)	Kec. (B/d)
1.	YA	118,7175	8.832,53
2.	YA	119,1451	8.800,83
3.	YA	119,8313	8.750,43
4.	YA	118,3828	8.857,50
5.	YA	119,4066	8.781,56
6.	YA	120,9556	8.669,10
7.	YA	119,4623	8.777,46
8.	YA	119,4012	8.781,96
9.	YA	119,6442	8.764,12
10.	YA	118,7175	8.832,53

Tabel 5. Sampel Percobaan Transfer Terenkripsi

Didapati nilai untuk kecepatan 8.738,52 B/detik (8,53 KiB/detik) dan nilai untuk keberhasilan 100 persen. Nilai kecepatan lebih kecil dari sambungan tunggal, yakni sebesar 3 (tiga) persen dari sambungan tunggal.

E. Jumlah Gerbang

Percobaan ini dilakukan untuk mengetahui hubungan antara jumlah sambungan dan jumlah Gerbang.

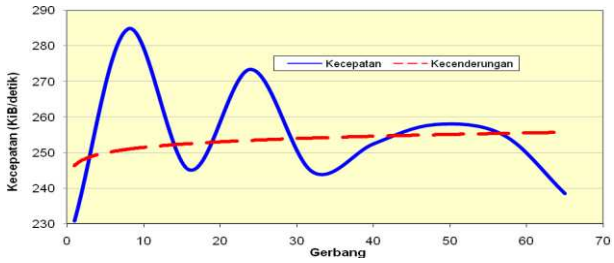
Dilakukan pengujian dengan melakukan serangkaian pengiriman sebanyak 50 kali dan dilakukan perhitungan rata-rata untuk kecepatan dan tingkat keberhasilan pengiriman berkas.

Lalu dilakukan pembandingan antara jumlah sambungan pengiriman dengan rata-rata kecepatan dan persen tingkat keberhasilan.

Gerb.	Berhasil	Persen Berhasil	Kec. (B/d)
1	50/50	100%	236.450,36
8	50/50	100%	236.450,36
16	50/50	100%	291.665,91
24	50/50	100%	251.078,29
32	50/50	100%	280.032,03
40	50/50	100%	250.579,63
48	50/50	100%	258.565,77
57	50/50	100%	264.073,65
65	50/50	100%	261.108,77

Tabel 6. Jumlah Gerbang.

Berikut ini adalah bagan tiap jumlah gerbang.



Gambar 11. Bagan Pembanding antara Kecepatan dan jumlah Gerbang.

Tingkat keberhasilan transfer adalah 100 persen. Dari bagan di atas, tampak bahwa jumlah Gerbang memiliki pengaruh terhadap kecepatan pengiriman dengan kecenderungan meningkat.

V. PENUTUP

A. Kesimpulan

Dari percobaan dan analisa tersebut, maka didapatkan beberapa kesimpulan sebagai berikut:

1. Pelompatan IP menggunakan soket untuk melaksanakan komunikasi antar-proses. Pelompatan IP memiliki tiga bagian utama, yakni Klien, Gerbang, dan Peladen. Klien berfungsi sebagai pengirim data, Gerbang berfungsi menjembatani antara Klien dan Peladen, dan Peladen berfungsi sebagai penerima data.
2. Pelompatan IP meningkatkan kerahasiaan dalam pengiriman data sebab memiliki nilai koefisien korelasi sebesar -0,00014 dibandingkan FTP sebesar 0 (nol) berdasarkan rumus Korelasi Diri.
3. Kecepatan pengiriman Pelompatan IP tertinggi adalah lebih lambat dari pada protokol pembanding, yakni FTP, sebesar 4,85 persen dari kecepatan FTP sebab pelompatan IP menggunakan pecahan-pecahan kecil sambungan dalam melakukan transmisi data sehingga memerlukan lebih banyak jabat tangan untuk membuka dan menutup sambungan.
4. Dari hasil pengujian, rata-rata waktu pengiriman tak terenkripsi tunggal adalah 291.665,91 B/detik (284,83 KiB/detik) dan 302.862,50 B/detik (295,76 KiB/detik) pengiriman tak terenkripsi paralel 2 (dua) sambungan dengan kecenderungan menurun untuk jumlah sambungan seterusnya.
5. Pengiriman terenkripsi RSA tunggal memiliki kecepatan 3 (tiga) persen dari kecepatan tanpa terenkripsi tunggal.

B. Saran

Terdapat beberapa saran untuk penelitian lebih lanjut, yaitu:

1. Penyempurnaan algoritma Pelompatan IP.
2. Pengiriman paralel dalam setiap waktu ke tujuan yang berbeda untuk penyebaran beban (*load balancing*).
3. Memperbaiki atau mengganti algoritma enkripsi dengan algoritma yang lebih baik.
4. Mengurangi jabat tangan TCP sehingga mengurangi waktu tunggu.
5. Memperbaiki pembacaan dan penulisan berkas sehingga mengurangi kesalahan data.

VI. RUJUKAN

1. United States Government Printing Office. 2012. *United States Code. Title 44: Public Printing And Documents. Subchapter III: Information Security* edisi 2012. http://www.gpo.gov/fdsys/pkg/USCODE-2012-title44/pdf/USCODE-2012-title44-chap35-subchapIII-sec3542.pdf (Diperbarui pada Senin, 09 Juni 2014, 16:07:06 WIB dan diakses pada Sabtu, 21 Juni 2014 08:41:13 WIB).
2. Cerf, Vinton G. dan Robert E. Kahn. 1974. "A Protocol for Packet Network Intercommunication" dalam *Communications, IEEE Transactions on* Volume 22 Terbitan 22, pada Mei 1974. New York: IEEE. http://ece.ut.ac.ir/Classpages/F84/PrincipleofNetworkDesign/Papers/CK74.pdf (Diperbarui pada Selasa, 21 Oktober 2003, 22:37:04 WIB dan diakses pada Kamis, 19 Juni 2014, 22:33:27 WIB).
3. IBM. -. How Sockets Work. http://www1.ibm.com/support/knowledgecenter/ssw_ibm_i_71/rzab6/howdosockets.htm (Diakses pada Jumat, 20 Juni 2014 09:51:54 WIB).
4. Rivest, Ronald L., dkk.. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" dalam *Communications of the ACM* Volume 2 terbitan 2 Februari 1978 halaman 120-126. New York: ACM. http://people.csail.mit.edu/rivest/Rsapaper.pdf (Berkas diperbarui pada Kamis, 26 April 2001 12:25:58 WIB dan diakses pada Minggu 22 Juni 2014 20:29:24 WIB).
5. Ullrich, Johannes. 2011. *Hashing Passwords*. http://www.dshield.org/diary/a/11110 (Publikasi pada 28 Juni 2011, diperbarui pada 28 Juni 2011 20:15:45 WIB, dan diakses pada Minggu, 22 Juni 2014 15:51:04 WIB).
6. Information Sciences Institute University of Southern California. 1981. *Transmission Control Protocol - DARPA Internet Program Protocol Specification*. Internet Engineering Task Force. RFC 793. https://tools.ietf.org/rfc/rfc793.txt (Berkas diperbarui pada Jumat, 16 Oktober 1992 04:56:43 WIB dan diakses pada Rabu, 04 Maret 2015, 22:23:12 WIB).
7. Filliben, James J. -. "Autocorrelation" dalam *NIST/SEMATECH e-Handbook of Statistical Methods*. Maryland: NIST Information Technology Laboratory. http://www.itl.nist.gov/div898/handbook/eda/section3/eda35c.htm (Berkas diubah pada Senin, 25 November 2013 23:20:36 dan diakses pada Senin, 23 Juni 2014 01:13:54 WIB)