RANCANG BANGUN APLIKASI UNTUK MENDETEKSI PERMASALAHAN JARINGAN KOMPUTER BERDASARKAN PAKET DATA PADA PROTOKOL TCP/IP MENGGUNAKAN ANALISIS OUTLIER

Imam Marzuki, Isbat Uzzin, M.Kom, MT, dan Nur Rosyid Mubtadai, S.Kom
Jurusan Informatika
Polteknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember (ITS) Surabaya
Kampus ITS Sukolilo Surabaya 60111
Email: marjuki@student.eepis-its.edu; isbat@eepis-its.edu; rosyid@eepis-its.edu

Abstrak (11 pt, bold)

Peningkatan kompleksitas jaringan komputer akan membutuhkan juga peningkatan kehandalan dari jaringan komputer tersebut sehingga perlu adanya deteksi dini terhadap permasalahan yang ada sebelum mempunyai pengaruh kepada user. Jika terjadi permasalahan, dari perspektif bisnis hal ini akan mengurangi pendapatan dan dari perspektif user hal ini akan memakan banyak waktu. Pada proyek akhir ini kami mencoba melakukan deteksi permasalahan jaringan berdasarkan paket data pada protokol TCP/IP. Metode pendeteksian mengunakan analisis outlier dimana akan ditentukan data yang mengalami fault dari sekumpulan data yang didapatkan. Diharapkan hal ini akan mendeteksi permasalahan di jaringan dan juga nantinya akan memberikan alert ke admin. Percobaan ini akan difokuskan pada proxy server.

Kata kunci: *TCP/IP, deteksi permasalahan jaringan, proxy server, data fault*

ABSTRACT

Increasing complexity of computer networks will also require increased reliability of the computer network so that the need for early detection of problems that existed before has the influence to the user. In case of problems, from a business perspective this will reduce revenues and from a user perspective it will take much time. At the end of this project we try to do the detection of network problems based on data packets on TCP / IP. Methods of data analysis using outlier analysis where the data have to be determined from a set of fault data obtained. It is hoped this will detect problems in the network and will also provide alerts to the admin. These experiments will be focused on the proxy server.

Keywords*: TCP/IP, detection network problems, proxy server, data fault*

1. Pendahuluan

Peningkatan kompleksitas jaringan komputer akan membutuhkan juga peningkatan kehandalan dari jaringan komputer tersebut sehingga perlu adanya deteksi dini terhadap permasalahan yang ada sebelum mempunyai pengaruh kepada user. Jika terjadi permasalahan, dari perspektif bisnis hal ini akan mengurangi pendapatan dan dari perspektif user hal ini akan memakan banyak waktu. Pada proyek akhir ini kami mencoba melakukan deteksi permasalahan jaringan berdasarkan paket data pada protokol TCP/IP. Metode pendeteksian menggunakan analisis outlier dimana akan ditentukan data yang mengalami fault dari sekumpulan data yang didapatkan. Diharapkan hal ini akan mendeteksi permasalahan di jaringan dan juga nantinya akan memberikan alert ke admin. Percobaan ini akan difokuskan pada proxy server.

Tujuan dari pendiagnosaan permasalahan jaringan tersebut adalah untuk memelihara kehandalan servis jaringan dengan cara mengidentifikasi permasalahan sebelum berdampak pada user.

Dalam proyek akhir ini kami berusaha melakukan deteksi permasalahan jaringan berdasarkan paper *"Fault Detection in IP-Based Process Control Networks using Data Mining* [7]. Parameter-parameter yang dijadikan acuan adalah beberapa paket-paket data pada protokol TCP/IP.

2. Teori Penunjang

2.1 Jaringan Komputer

Kebutuhan akan adanya suatu jaringan informasi meningkat dengan pesat. Kebutuhan kita akan informasi bertambah besar. Bagi sebagian masyarakat, informasi telah menjadi barang kebutuhan primer, dan hal tersebut berkaitan erat dengan perkembangan dunia jaringan komputer.

Sebelum era penggunaan jaringan komputer, penggunaan komputer sangat terbatas untuk mesin-mesin *standalone* yang terpisah dan *independent* antara satu dengan yang lainnya. Tetapi setelah memasuki era penggunaan jaringan, kumpulan komputer-komputer *standalone* tersebut dihubungkan satu dengan yang lainnya dan menjadi suatu jaringan sehingga seluruh informasi dari masing-masing komputer dapat dikorelasikan. Beberapa tujuan dari penggunaan jaringan komputer :*Resources sharing*, *Reliabilitas* atau kahandalan yang tinggi, biaya, dan *skalabilitas*

2.2 Deteksi Fault dan Diagnosis

Berdasakan [4] [5] [6] [7], definisi dari fault adalah cacat dalam kualitas. Sedangkan definisi failure menurut [3] adalah performa atau kinerja kurang memuaskan.

Berikut ini adalah beberapa fault dan failure serta penyebabnya:

- *IP connectivity errors* : stabil transmisi, throughput rendah, delay, jaringan ancaman sequrity, manajemen sumber daya IP.
- *Network mis-configuration* **:** jaringan topologi loop, jalur yang optimal (non redundansi), ketidakcocokan dupleks.
- *Physical defects* : kerusakan hardware, link korupsi (kerusakan kabel), gangguan listrik, pemadaman listrik, menduplikasi alamat hardware.
- *Software defects* : Pemrograman PLC bug, bug perangkat driver, ketidaksadaran protocol.

3. Perancangan dan Implementasi

3.1 Spesifikasi Aplikasi

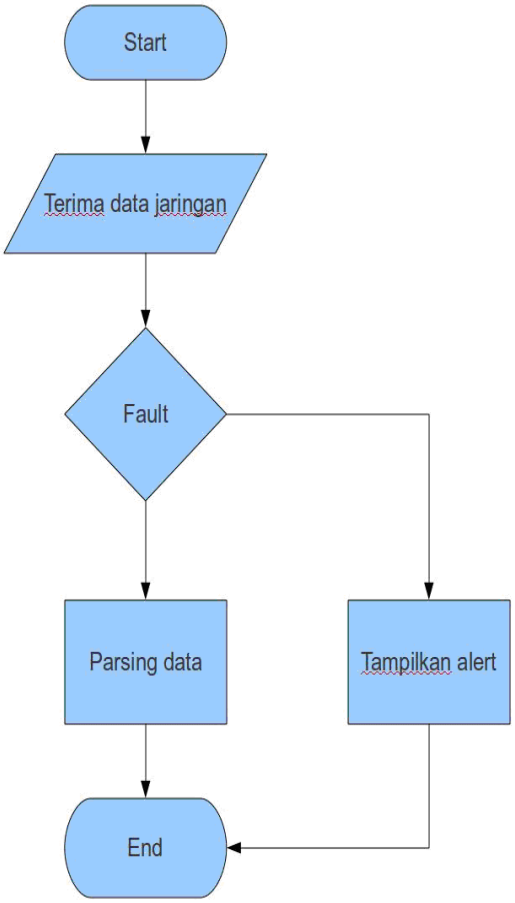
Sebelum melakukan proses pembuatan aplikasi, terlebih dahulu ditentukan spesifikasi aplikasi. Spesifikasi aplikasi akan menjadi titik tolak sekaligus menjadi acuan untuk pembuatan aplikasi dan juga menentukan kapabilitas dan kemampuan apa saja yang harus bisa dipenuhi sistem tersebut.

Aplikasi yang dibangun memiliki spesifikasi sebagai berikut:

- Aplikasi beroperasi pada platform Windows
- Aplikasi yang digunakan harus bisa mengambil data-data dari jaringan.
- Semua data yang telah dicapture disimpan dalam bentuk file.
- Aplikasi harus bisa mendeteksi permasalahan pada data hasil capture.

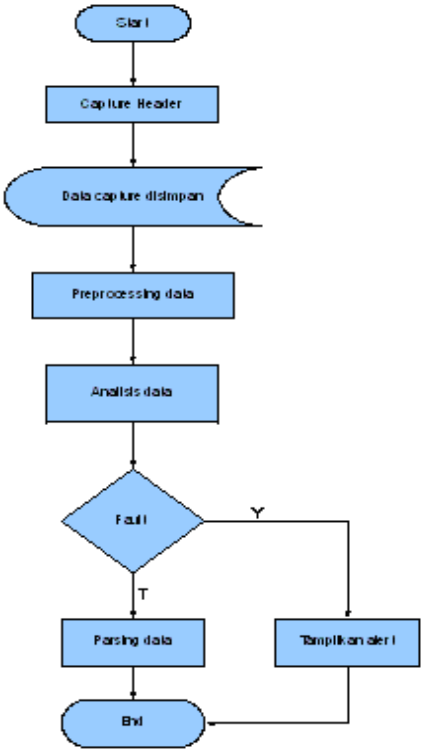
3.2 Desain Sistem Secara Umum

Secara umum aplikasi yang akan dibangun adalah sebagai berikut.



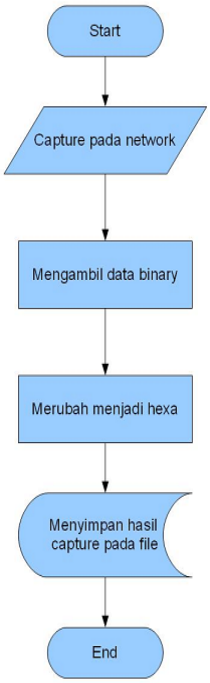
Gambar 1. flowchart desain system secara umum

3.3 Desain Pendeteksian Data Fault



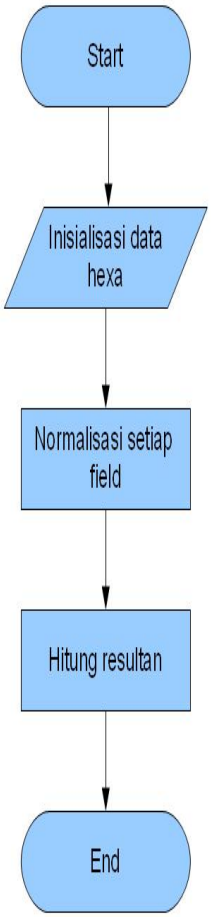
Gambar 2. flowchart pendeteksian data fault

3.4 Desain Pengambilan Data



Gambar 3. flowchart desain pengambilan data

3.5 Desain Preprocessing Data



Gambar 4. flowchart desain preprocessing data

3.5.1 Perhitungan Normalisasi

Data akan digunakan range data berkisar dari 0 hingga 1. untuk itu digunakan perumusan matematika seperti persamaan dibawah.

$$Normalisasi = \frac{d}{d\max}$$

Persamaan 1. Rumus normalisasi

3.5.2 Perhitungan Resultan

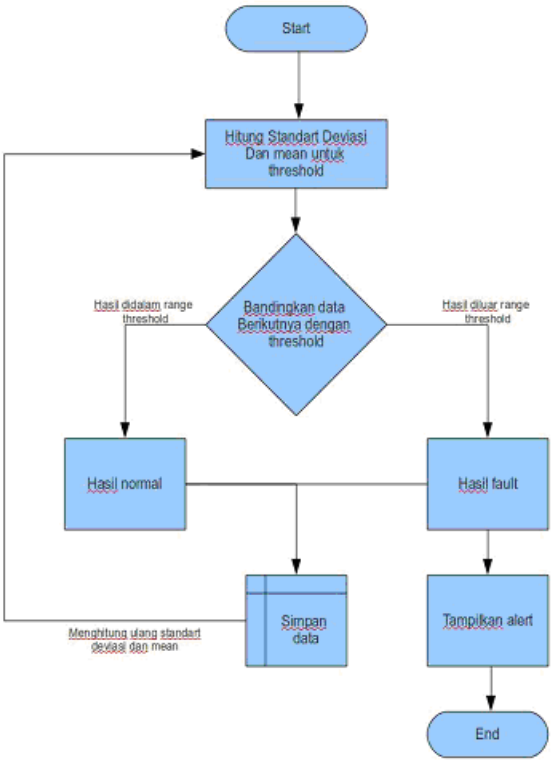
Setelah kita mendapatkan data normalisasi dari setiap field pada ip header maka kita akan menghitung resultan dari nilai-nilai tersebut, karena terdiri dari beberapa data maka bisa dikatakan datanya multi dimensi. Berikut ini rumus untuk menghitung resultannya.

$$R = \sqrt{dataX^2 + datY^2 + datZ^2 + ...}$$

Persamaan 2. Rumus mencari nilai resultan

3.6 Desain Analisis Data

Analisis data adalah proses setelah kita mendapatkan nilai resultan dari setiap field yang ada pada ip header. Dari data tersebut kita bisa memperoleh standart deviasi dan rata-rata dari nilai keseluruhan data, sehingga kita dapat mengetahui nilai thresholdnya. Jika sebuah data berada di luar threshold maka data tersebut akan dianggap fault oleh aplikasi. Disini semua data baik data yang dianggap anomaly atau data normal akan disimpan dalam sebuah array/vector, aplikasi akan menghitung ulang nilai standart deviasi dan rata-ratanya setiap interval tertentu yang kita inginkan. Berikut ini flowchart proses dari analisis data.



$$StadartDeviasi = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(d-\overline{d})^2}$$

Persamaan 3. Rumus mencari standart deviasi

$$Threshold = mean \pm 2 * StadartDeviasi$$

Persamaan 4. Rumus menentukan threshold

4. Ujicoba dan Evaluasi

Pada bab ini akan dibahas mengenai pengujian terhadap aplikasi. Pertama-tama akan dibahas mengenai uji terhadap data offline (data tidak realtime) lalu uji terhadap data online (data

realtime), kemudian dijabarkan pula bagaimana penulis melakukan pengujian tersebut. Setelah itu pembahasan berlanjut ke hasil pengujian.

Uji coba ini bertujuan untuk mengetahui apakah aplikasi berjalan sesuai dengan kebutuhan sistem dan fungsi yang telah diuraikan pada Bab III.

4.1 Uji Data Offline (data tidak realtime)

Pada pengujian ini digunakan data offline yang terdiri dari data fault yang berasal dari sebuah instansi terpercaya sebagai validitas dari kehandalan aplikasi, disini data fault merupakan data attack. Data attack diambil dari DARPA 1999. Data set DARPA 1999 merupakan data packet yang dicapture pada jaringan selama 22 jam oleh MIT Lincolin Laboratory. Dari sekian banyak data DARPA 1999 diambil data training week 1-monday sebagai sampel. Dalam hal ini data serangan digabungkan dengan data normal dengan prosentase yang berubah-ubah. Sedang data normal adalah data yang tidak terbukti teridentifikasi fault.

. Pengujian ini bertujuan untuk mengetahui kehandalan aplikasi untuk mendeteksi adanya data fault dan data normal. Pada pengujian ini terdapat kriteria yang menjadi acuan yaitu:

1. TP (True Positif), yakni data fault yang terdeteksi fault
2. FP (False Positif), yakni data normal yang terdeteksi fault.
3. FN (False Negatif), yakni data normal yang terdeteksi normal.

Dari ketiga criteria tersebut dapat ditentukan tingkat keberhasilan

$$TingkatKeberhasilan = \frac{TP}{TP + FP} * 100\%$$

Persamaan 5. Rumus tingkat keberhasilan

Dari hasil uji coba terhadap beberapa data DARPA 1999 didapatkan informasi sebagai berikut.

Tabel 1 Hasil Pengujian terhadap beberapa campuran data normal dan data fault

Data	Prosentase Data		Prosentase Hasil Deteksi	
	Normal	Fault	Keberhasilan	Kegagalan
50	45 %	5 %	93 %	7 %
50	40 %	10 %	85 %	15 %
100	97 %	3 %	87 %	13 %

4.2 Uji Data Online Pertama (data bebas)

Untuk pengujian online (data bebas) dilakukan pada waktu penulis terkoneksi secara bebas ke internet sambil melakukan browsing. Pada pengujian ini akan diambil data secara acak dalam jumlah tertentu secara random. Berikut ini hasil pengujian terhadap data online (data bebas):

Tabel .2 Hasil Pengujian terhadap beberapa data bebas pada saat penulis browsing

No	Data	Terdeteksi	Tingkat Keberhasilan (%)
1.	50	12	24 %
2.	100	17	17 %

Dimana :

$$TingkatKeberhasilan = \frac{Ter\det eksi}{JumlahData} * 100\%$$

Persamaan 6 Rumus tingkat keberhasilan data online bebas

4.2 Uji Data Online kedua (data realtime)

Untuk pengujian online (data realtime) akan dilakukan pada sebuah network yang terkoneksi pada proxy server, disini data yang melewati jaringan berupa data yang berasal dari internet/intranet. Dalam hal ini data fault yang dijadikan sampel adalah data hasil scanning, data pemutus jaringan dan data serangan. Fault akan dilakukan dengan sebuah PC di dalam network dengan menggunakan tool vurnerability scanner, network cut, dan exploit. Dalam pengujian ini tool tersebut adalah Superscan (Scanner Jaringan), Netcut (Pemutus Jaringan), Lan Attacker / WinArp Attacker (Software serangan). Masing-masing tool akan memberikan berbagai jenis penetrasi yang berbeda kepada komputer yang terpasang aplikasi pendeteksi ini. Pada saat test semua aplikasi anti virus dan firewall dimatikan.

Dimana :

$$TingkatKeberhasilan = \frac{Ter\det eksi}{JumlahData} * 100\%$$

Persamaan 7. Rumus tingkat keberhasilan data online realtime

Tabel 3 Hasil Pengujian terhadap beberapa data yang mengalami scanning (dengan software supercan)

No	Data	Terdeteksi	Tingkat Keberhasilan (%)
1.	50	14	28 %
2.	100	19	19 %

Tabel 4 Hasil Pengujian terhadap beberapa data yang diberi pemutus jaringan (dengan software net cut)

No	Data	Terdeteksi	Tingkat Keberhasilan (%)
1.	50	11	22 %
2.	100	24	24 %

Tabel 5 Hasil Pengujian terhadap beberapa data yang diberi serangan (dengan software LAN Attacker)

No	Data	Terdeteksi	Tingkat Keberhasilan (%)
1.	50	48	96%
2.	100	97	97%

5. Penutup

Bab ini menyimpulkan hasil uji coba yang telah dilakukan. Selanjutnya diberikan beberapa saran yang mungkin dapat dijadikan pertimbangan untuk mengembangkan hasil yang diperoleh pada tugas akhir ini.

5.1 Kesimpulan

Dari pengujian sistem yang ada maka dapat diambil kesimpulan bahwa sistem yang dibuat memiliki keunggulan sebagai berikut :

1. Sistem dapat mengambil data pada network yang aktif sehingga semua data bisa dilihat apakah data itu merupakan data yang dibutuhkan atau tidak.
2. Sistem mampu mendeteksi dengan baik apakah data yang masuk merupakan data fault atau tidak.

5.2 Saran

Dari kesemua kegiatan yang sudah dilakukan mulai awal hingga akhir, maka muncul saran dari penulis yang seharusnya dilakukan di masa yang akan datang. Saran-saran itu adalah: Peningkatan akurasi aplikasi dalam mengenali data yang termasuk fault bisa diperluas lagi cakupannya sehingga dapat dijadikan acuan untuk mendiagnosa suatu permasalahan jaringan dengan lebih akurat.

Daftar Pustaka

1. Putra, Wijaya M. *Perancangan dan Pembuatan Program Deteksi Intrusi Pada Jaringan Komputer Berdasarkan Packet Header Dengan Analisis Outlier*. Proyek Akhir D4 Teknik Informatika PENS-ITS 2010
2. Ahmad Fajar al Kharis. *Deteksi Intrusi Pada Jaringan Komputer Berdasarkan Analisa Payload Menggunakan Metode Outlier*. Proyak Akhir D3 Teknik Informatika PENS-ITS 2010
3. Amy Ward, Peter Glynn, dan Kathy Richardson. *Internet Service Failure Detection*
4. Roy A. Maxion dan Robert T. Olszewski. *Detection and Discrimination of Injected Network Faults*
5. Frank Feather, Dan Siewlorek, dan Roy Maxion. *Fault Detection in an Ethernet Network Using Anomaly Signature Matching*
6. Roy A. Maxion. *Anomaly Detection for Diagnosis*

7. Byungchul Park, Young J.Won, Hwanjo Yu, James Won-Ki Hong, Hong-Sun Noh, and Jang Jin Lee. *Fault Detection in IP-Based Process Control Networks using Data Mining*

8. 1999 DARPA intrusion detection evaluation data set. http://www.ll.mit.edu/mission/communications/ist.corpora/ideval/data/1999/training/week1/index.html