Penentuan Anomali Paket Data Jaringan Menggunakan Metode *Outlier*

Imam Marzuki

Program Studi Elektro, Fakultas Teknik, Universitas Panca Marga
Jl. Yos Sudarso 107 Pabean Dringu Probolinggo 67271
Email : imammarzuki32@gmail.com

Terima Naskah : 20 Agustus 2015
Terima Revisi : 5 September 2015

ABSTRAK

Seiring dengan semakin berkembangnya teknologi internet, kejahatan yang memanfaatkan teknologi ini juga semakin meningkat. Hal ini ditambah lagi dengan semakin banyaknya peredaran aplikasi gratis yang dapat digunakan untuk melancarkan usaha pembobolan suatu sistem berbasis teknologi jaringan internet. Pada penelitian ini kami mencoba melakukan penentuan anomali paket data jaringan pada protokol IP. Metode penentuan mengunakan metode *outlier* dimana akan ditentukan data yang mengalami anomali dari sekumpulan data yang didapatkan. Diharapkan hal ini akan memberikan deteksi dini bahwa ada masalah di jaringan dan juga nantinya akan memberikan peringatan berupa SMS ke admin.

Kata kunci: *IP, metode outlier, paket data anomali*

ABSTRACT

Along with the development of Internet technology, crimes using this technology have also increased. This is coupled with the increasing circulation of free applications that can be used to launch a business break-ins internet network technology based systems. In this study we tried to determine anomalies in the network data packets IP protocol. The method of determining the method to be determined where the data outlier who experienced an anomaly of a set of data obtained. It is hoped this will provide early detection that there is a problem in the network and also will give a warning SMS to admin.

***Keywords**: IP, outlier method, data packets anomaly*

PENDAHULUAN

Kebutuhan bisnis dan aktivitas yang cukup banyak membuat hampir sebagian besar operasional dilakukan secara daring (*online*). Kita sering melihat perusahaan yang menjual produknya tidak hanya secara fisik, namun juga secara daring, termasuk transaksi pembayarannya. Gambaran tersebut menunjukkan bahwa teknologi internet menjadi pilar utama dalam operasional perusahaan atau institusi tersebut.

Seiring dengan bertambahnya kebutuhan perusahaan atau institusi atas jaringan internet untuk transaksi, kegiatan-kegiatan yang bertujuan jahat seperti *deface* atau pencurian data yang dilakukan oleh orang yang tidak bertanggung jawab juga meningkat. Kejahatan ini sering dilakukan dengan memanfaatkan jalur jaringan komputer. Orang-orang yang tidak bertanggung jawab ini melakukan pencurian atau perusakan sistem dengan perkakas (*tool*) tertentu. Secara teori, walaupun orang-orang ini sudah menghapus jejaknya, baik log data maupun log lainnya, kita tetap dapat menganalisis beberapa data yang mungkin ditinggalkan sistem jaringan lainnya. Salah satunya adalah penentuan anomali paket data dalam jaringan.

Dalam penelitian ini kami berusaha melakukan penentuan anomali paket data jaringan berdasarkan paper "*Anomali Detection in IP-*

Based Process Control Networks using Data Mining [7]. Parameter-parameter yang dijadikan acuan adalah beberapa paket-paket data pada protokol IP.

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*

Definisi Anomali

Berdasakan [4] [5] [6] [7], definisi dari anomali adalah cacat dalam kualitas. Berikut ini adalah beberapa anomali 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.

METODE

Spesifikasi Aplikasi

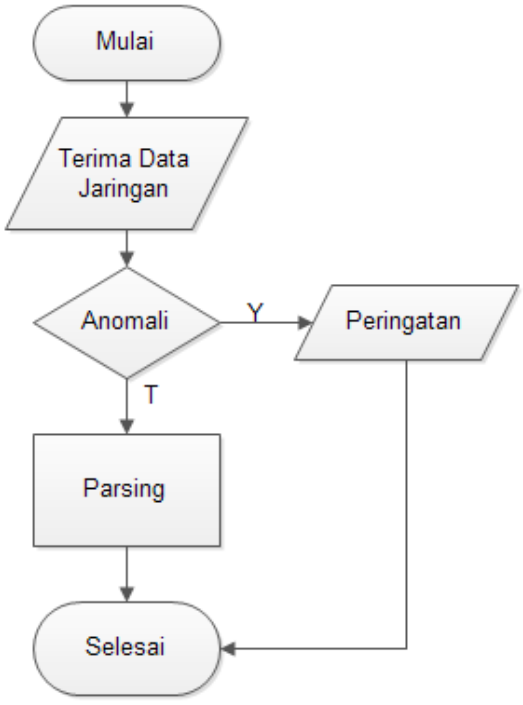
Sebelum melakukan proses pembuatan aplikasi, terlebih dahulu ditentukan spesifikasi aplikasi. Spesifikasi aplikasi akan menjadi titik tolak sekaligus menjadi acuan untuk pembuatan aplikasi dan juga menentukan kapabilitas dan kemampuan apa saja yang harus bisa dipenuhi sistem tersebut.

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.

Desain Sistem Secara Umum

Secara umum aplikasi yang akan dibangun adalah sebagai berikut :



Gambar 1. flowchart desain sistem secara umum

Pada gambar 1 diatas, input dari program adalah data jaringan yang masuk kemudian akan di proses apakah data mengalami anomali apa tidak. Jika data yang datang adalah data anomali maka aplikasi akan menampilkan alert/peringatan bahwa

data ada masalah / anomali. Jika tidak ada masalah / anomali, maka data akan diteruskan.

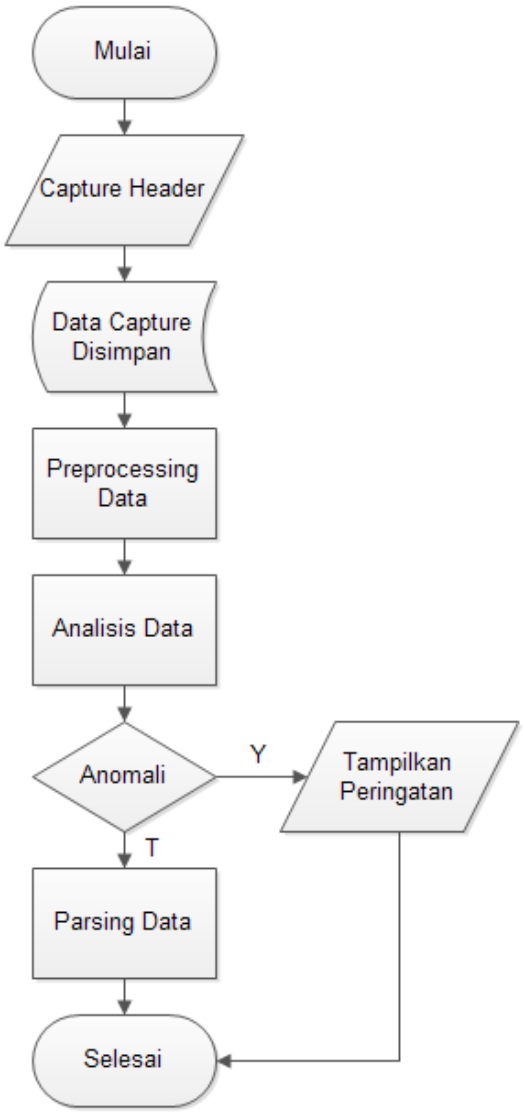
Desain Pendeteksian Data Anomali

Apabila kita menggunakan sistem operasi berbasis windows sebagai router tentunya hal tersebut tidak bisa dilakukan secara langsung. Karena kita harus mengambil data dari paket tersebut secara detail, walaupun yang akan kita ambil hanya sebatas header dari data. Bukan keseluruhan dari paket tersebut untuk menjaga privasi user dari server. Dengan demikian kita perlu menempatkan aplikasi WinPcap sebagai sniffer untuk memperoleh header dari data itu.

Data yang akan masuk dibelokkan terlebih dahulu untuk diambil datanya sebelum dilanjutkan ketujuan sebenarnya. Didalam pembelokan ini tidak berarti bahwa data paket ditahan dulu untuk diteliti melainkan data yang dating maupun keluar hanya di capture headernya.

Dengan mengetahui header dari setiap paket yang masuk dapat kita peroleh data-data dari paket, yang kemudian kita bisa mengklasifikasikan setiap data yang dating apakah itu paket TCP, UDP atau juga ICMP. Beserta semua keterangan darimana paket itu berasal, kemana tujuannya, juga besar dari paket tersebut.

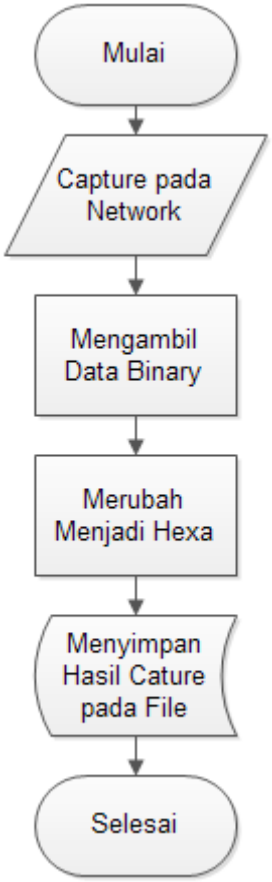
Untuk desain pendeteksian data anomali, secara garis besar digambarkan dalam flowchart berikut ini :



Gambar 2. flowchart pendeteksian data anomali

Desain Pengambilan Data

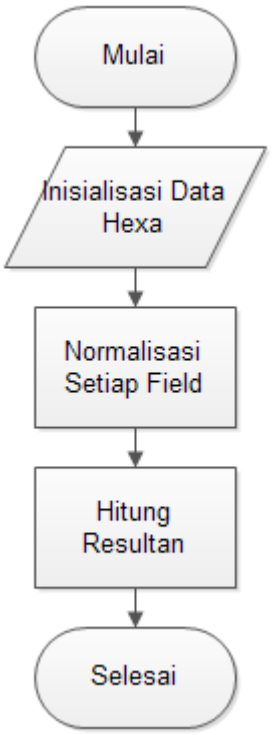
Data yang akan masuk di belokkan terlebih dahulu untuk diambil datanya sebelum dilanjutkan ketujuan sebenarnya. Didalam pembelokan ini tidak berarti bahwa data paket ditahan dulu untuk diteliti melainkan data hanya yang datang maupun keluar di capture headernya.



Gambar 3. flowchart desain pengambilan data

E. Desain Preprocessing Data

Setelah melakukan capture data dan menyimpan data capture tersebut pada file maka pada aplikasi akan dilakukan analisis data hexa yang telah dicapture tersebut. Yang dimaksud preprocessing data sendiri terdiri dari dua proses yaitu normalisasi data dan perhitungan resultan.Tidak semua data akan diproses, data yang diproses antara lain source IP address, destination IP address, source port number, destination port number, protocol, total bytes, ip checksum, tcp checksum, dan tcp flag (tcp SYN flag, tcp FIN flag, tcp ACK flag, tcp RST flag, tcp URG flag, tcp PSH flag). Berikut flowchart dari preprocessing data:



Gambar 4. flowchart desain preprocessing data

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

$$Normalisasi = \frac{d}{d\ \max} \qquad (1)$$

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.

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

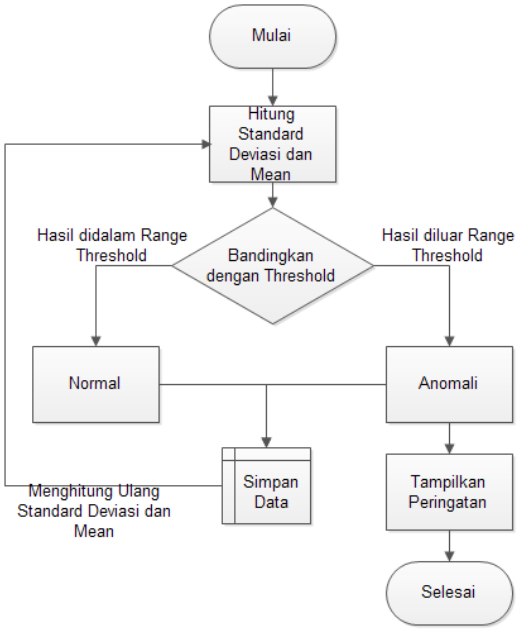
F. Desain Analisis Data

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.

$$StadartDeviasi = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(d-\bar{d})^2} \quad (3)$$

$$Threshold = mean \pm 2 * StadartDeviasi \quad (4)$$

Jika sebuah data berada di luar threshold maka data tersebut akan dianggap anomali 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.



Gambar 5. flowchart desain analisis data

HASIL DAN PEMBAHASAN

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 sub pokok bahasan sebelumnya.

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):

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 anomali yang dijadikan sampel adalah data hasil scanning, data pemutus jaringan dan data serangan. Anomali 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 :

$$TingkatKeberhasilan = \frac{Terdeteksi}{JumlahData} * 100\% \quad (5)$$

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%

SIMPULAN

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 anomali atau tidak.

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*. Proyek 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 Anomalis*

[5] Frank Feather, Dan Siewlorek, dan Roy Maxion. *Anomali 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. *Anomali Detection in IP-Based Process Control Networks using Data Mining*

[8] 1999 DARPA intrusion detection evaluation data set.