APLIKASI MOBILE UNTUK K-NEAREST NEIGHBOR PADA INTRUSION DETECTION SYSTEM BERBASIS SNORT

Novi Anisyah[1], Moch Zen Samsono Hadi[2], Entin Martiana K.[3]
Jurusan Telekomunikasi, Piliteknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember (ITS) Surabaya
Kampus PENS-ITS, Keputih, Sukolilo, Surabaya.
novianisyah@student.eepis-its.edu

Abstrak - Mencocokan pola/signature adalah metode yang paling umum untuk mendeteksi serangan dan ini berarti IDS harus mampu mengenali setiap teknik serangan supaya menjadi efektif. IDS memiliki database yang besar dengan ribuan signature yang memungkinkan IDS mencocokan signature atau pola serangan. Respon otomatis yang biasanya dilakukan adalah menyalakan alarm dengan mencatat di-log , mengirim email atau memblok serangan. Kelemahan respon otomatis yang umum adalah terjadinya respon terhadap false negative dan false positive. Adalah penting untuk memahami mengapa signature memicu dan mengidentifikasi true dari false positive.
Pengunaan algoritma nearest neighbor dilandasi oleh pemikiran perlu adanya solusi terhadap nilai anggota bilangan atau membership value (MV) yang tidak hanya berorientasi pada benar atau salah, terpenuhi (MV=1) , atau tidak terpenuhi (MV=0). Algoritma nearest neighbor ini nantinya akan diletakkan pada metode pembacaan signature/pola tertentu dari suatu paket serangan yang umum. Sehingga Algoritma k-Nearest neighbor menjadi kecerdasan buatan yang digunakan sebagai Pattern Recognition pada SNORT IDS.Hasil dari pengujian dari data real-time di jaringan dan data serangan akan didefinisikan.Dan di tampilkan dalam bentuk web menggunakan PHP-AJAX dan dapat di akses melalui aplikasi mobile.
Pengunaan algoritma nearest neighbor pada tugas akhir ini telah mampu untuk mengklasifikasikan scanning jenis TCP Xmas Tree scan (-sX) 93.4% dan 100% ping of Death (POD) kedalam kategori serangan.waktu yang dibutuhkan utuk akses k-NN engine melalui mobile device yang paling bagus adalah pagihari yaitu dengan waktu rata-rata 4s.

Kata kunci : IDS, Nearest Neighbor, SNORT,Scanning.

1. PENDAHULUAN

Salah satu upaya melindungi jaringan dari ancaman-ancaman hacker adalah membangun Sistem Deteksi Intrusi atau Intrusion Detection System (IDS) pada jaringan tersebut. Secara berkala vendor IDS akan merilis signature untuk serangan-serangan baru dan menjadi tugas Network Administrator untuk men-deploy signature tadi kedalam IDS yang ada pada jaringan nya. Masalah muncul ketika serangan-serangan baru muncul dalam interval waktu yang relatif cepat, network administrator tidak bisa sepenuhnya berharap kepada vendor IDS untuk membuat signature yang baru dalam kurun waktu yang singkat, sehingga seorang network administrator harus membuat signature sendiri dan tetap update terhadap jenis-jenis serangan baru yang muncul.

Mengingat beban pekerjaan network administrator yang besar dan luas, sangat tidak mungkin seorang network administrator untuk selalu update tiap waktu terhadap serangan-serangan baru dan dengan singkat membuat signature untuk serangan baru tersebut. Maka muculah ide bagaimana membuat suatu sistem deteksi intrusi baru yang dapat mengenali pola serangan baru dari serangan-serangan lama yang sudah ada dan secara otomatis membuat signature untuk serangan tersebut dan menambahkannya kedalam rule yang ada pada IDS tersebut. Sistem ini kemudian dikenal dengan nama

Intelligence Intrusion Detection System (IIDS) dimana secara sengaja memasang suatu kecerdasan buatan (Artificial Intelligence) kedalam Intrusion Detection System (IDS).

Pada Penelitian Proyek Akhir ini, dibuat suatu Intelligence Intrusion Detection System (IIDS) dimana Algoritma k-Nearest neighbor menjadi kecerdasan buatan yang digunakan sebagai Pattern Recognition dan di implementasikan pada SNORT IDS.

Beberapa permasalahan yang akan dibahas dalam penelitian proyek akhir ini, diantaranya :

1. Bagaimana mengenerate database log dari snort, yang selanjutnya digunakan sebagai data serangan.
2. Bagaimana mengklasifikasi Network Package baru kedalam Attack Package atau Normal Package menggunakan Algoritma Nearest neighbor
3. Membuat Interface dalam bentuk Web yang akan meng-integrasikan SNORT dengan Nearest neighbor Engine
4. Bagaimana mengakses/memantau sistem yang telah dikerjakan dengan menggunakan aplikasi mobile

Batasan masalah yang harus diselesaikan pada penelitian ini adalah:

a. Data serangan yang dipakai hanya yang berasal dari Log Database milik SNORT
b. Atribut dari Network Package yang digunakan hanya 4 yaitu Protokol, Destination Port, Flag dan Size
c. Implementasi dan uji coba dilakukan pada jaringan lokal.

2. DASAR TEORI

Beberapa materi pustaka yang mendukung perancangan dan pembuatan Aplikasi Mobile Untuk Metode K-Nearest Neighbor Pada Intrusion Detection Sistem Berbasis Snort. Materi – materi tersebut meliputi : Intrusion Detection System dan k-Nearest Neighbor.

2.1 IDS (Intrusion Detection Sistem)

IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

2.2 Jenis-jenis IDS

Ada dua jenis IDS, yakni:

a. Network-based Intrusion Detection System (NIDS)

   Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch Ethernet sekarang telah menerapkan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.

b. Host-based Intrusion Detection System (HIDS)

   Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.

Tipe dasar IDS adalah:

a. Rule-based system : berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalulintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.
b. Adaptive system : mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada. Tapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk penyusupan yang baru.

Snort

Snort dapat dioperasikan dalam 3 mode yaitu :

a. Sniffer mode, untuk melihat paket yang lewat di jaringan.
b. Logger mode, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
c. Intrusion Detection Mode, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini diperlukan setup dari berbagai file atau aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

2.4 Logika k-Nearest Neighbor

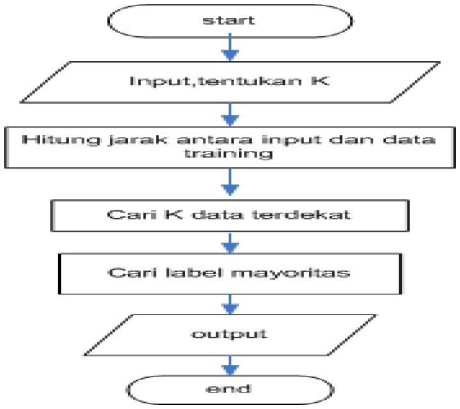
Algoritma k-nearest neighbor (k-NN atau KNN) adalah sebuah metode untuk melakukan klasifikasi terhadap objek berdasarkan data pembelajaran yang jaraknya paling dekat dengan objek tersebut.

k-nearest Neighbor merupakan metode klasifikasi instance-based, memilih satu objek latih yang memiliki sifat ketetanggaan (neighborhood) yang paling dekat. Sifat ketetanggaan ini didapatkan dari perhitungan nilai kemiripan ataupun ketidakmiripan.

KNN menggunakan metode perhitungan nilai ketidakmiripan (Euclidian, Manhattan, Square Euclidian ,dll). KNN akan memilih K-tetangga terdekat untuk menentukan hasil klasifikasi dengan melihat jumlah kemunculan dari kelas dalam K-tetangga yang terpilih. Kelas yang paling banyak muncullah yang akan menjadi kelas hasil klasifikasi.

Rumus Euclidian:

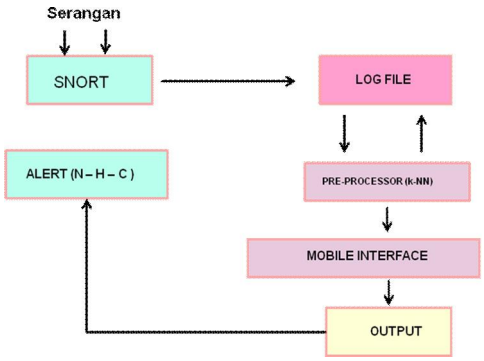
$$\text{jarak} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$



Gambar1. Flowchart k-NN

Pada Gambar 1 Setelah snort dijalankan. Sistem mendapatkan inputan berupa data serangan dari snort. kemudian tentukan jumlah K. K disini adalah positive integer, yang menentukan jumlah tetangga terdekat. Kemudian Hitung jarak antara data baru ke setiap label data pada data training .Lalu Tentukan k labeled data yang mempunyai jarak terdekat selanjutnya klasifikasikan data baru terhadap label data mayoritas.

3. RANCANGAN SISTEM



Gambar 2. Diagram alur dari K-nearest neighbor Intrusion Recognition Engine

Data log yang berhasil di capture oleh SNORT dihitung jaraknya terhadap data training, lalu hasil di tampilkan pada user interface yang menggunakan PHP dan Ajax yang secara realtime akan selalu meng-update rules SNORT jika ada serangan baru yang nantinya akan dilakukan action dengan memblokir

nomer IP yang digunakan untuk melakukan serangan.

4. HASIL YANG DIKERJAKAN

Dari perancangan sistem yang telah dibuat, telah dilakukan beberapa pengamatan dan uji coba scanning dengan menggunakan beberapa tipe data yaitu data normal(HTTP,TELNET),Scanning DOS dan IP Spoofing dengan jumlah k dinamis dari 1 sampai 10.dan jumlah database yang berubah-ubah dari 30,60,90,120 dan 257.

4.1 Percobaan k-Nearest Neighbor

Untuk percobaan k-nerest neighbor juga dilakukan labelisasi dan dibandingkan dengan snort.

Tabel2. Perbandingan snort dan knn

SERANGAN	SNORT ALERT (%)		K-NN (100%)		
	S	BS	S	BS	T
SCANNING *)					
connect scan (-sT)	100	0	-	-	100
TCP SYN scan (sS)	100	0	-	-	100
TCP FIN scan (-sF)	100	0	19.75	80.04	0.21
TCP Xmas Tree scan (-sX)	98.28	1.72	93.44	6.28	0.28
TCP Null scan (-sN)	100	0	50	25	25
TCP ACK scan (-sA)	100	0	-	-	100
UDP scan (-sU)	27.4	72.6	-	53.23	46.77
-sP	-	-	-	-	-
-O	78.6	21.4	14.28	28.68	57.04
DoS *)					
POD	87.03	12.97	87.03	12.97	0
Data Normal *)					
telnet	0	100	0	35.29	64.71
Ssh	-	-	-	-	-
http	0	100	14.28	85.71	0.01
ftp	-	-	-	-	-
IP SPOOFING *)					
pod_spoof	-	-	-	-	-
syn_flood	97.8	2.2	70.75	25.74	3.51
land_attack	99.4	0.6	Error	error	Error

Ket: s: Serangan
BS: Bukan serangan
T:Tidak terdeteksi

Dari tabel terlihat bahwa k-nn juga sudah bekerja sangat baik untuk jenis scanning xmas scan 93,44% serangan yang ada telah terklasifikasi.begitu juga POD seluruh serangan yang ada di snort telah terklasifikasi yaitu 87.03%.namun system ini belum bisa bekerja untuk jenis serangan yang mengirimkan paket data sangat besar seperti land_attack.

4.2 Perbandingan fuzzy dan knn

Disini dilakukan perbandingan label hasil fuzzy dan k-nearest neighbor

Tabel3.perbandingan fuzzy dan knn

SERANGAN	Fuzzy(%)				k-NN (%)			
	H	C	N	UC	H	C	N	U
SCANNING *)								
connect scan (-sT)	-	-	-	-		-	-	-
Ss (TCP SYN scan)	-	-	-	-		-	-	-
TCP FIN scan (-sF)	20,09	0,00	79,91	0	19.78	0	80.22	-
TCP Xmas Tree scan (-sX)	91,12	7,16	1,72	0	84.24	9.45	6.31	-
TCP Null scan (-sN)	66,67	0,00	33,33	0	66,66	0	33.4	-
TCP ACK scan (-sA)	33,33	66,67	0,00	0				-
UDP scan (-sU)	0,00	0,00	100,00	0	0	0	100	-
-sP	-	-	-	-	-	-	-	-
-O	50	50	100,00	0	33,33		66,66	-
DoS *)								
POD	-	0	12.97	0	87.03	0	12.97	-
Data Normal *)								
telnet	0,00	0,00	100,00		0	0	100	-
Ssh	-	-	-		-	-	-	-
http	0,00	14,29	85,71		7.14	0	92.86	-
ftp	-	-	-	-	-	-	-	-
IP SPOOFING *)								
pod_spoof	-	-	-	-	-	-	-	-
syn_flood	49,62	48,11	2,27	-	0	73.29	26.71	-
land_attack	99,42	0,00	0,58	-		-	-	-

Pada tabel terlihat fuzzy dan knn sudah sama-sama nekerja dengan baik pada scanning xmas scan fuzzy mendeteksi 92.57% sedangkan knn 93,44% untuk POD fuzzy tidak bekerja dengan baik karena banyak data yang tidak terclasifikasi,sedangkan pada k-nn

bekerja dengan sangat baik 100% serangan yang ada telah terdeteksi.untuk jenis serangan land_attack fuzzy sudah mmapu mendeteksi 100% serangan yang ada.jika pada k-nn untuk seragan ini masih belum mampu memproses karena data yang begitu besar.

4.3 Perbandingan Hierarcical clustering,k-Nearest neighbor dan fuzzy neural network

Untuk perbandingan 3 metode Hierarcical clustering,k-Nearest neighbor dan fuzzy neural network.dibagi menjadi 2 yaitu perbandingan label dan perbandingan waktu komputasi.

Tabel 4.perbandingan label 3 metode

Serangan	Hierarchical Clustering (%)			K-Nearest Neighbor (%)			Fuzzy Neural Network (%)		
	N	H	C	N	H	C	N	H	C
FIN Scan	5	2	0	19,78	0	80,22	78,36	21,6	0
XMAS Scan	0	4	96	6.31	84.24	9.45	15,18	84,81	0
NULL Scan	100	0	0	33.4	66,66	0	33,33	66,66	0
Ping of Death	99	1	0	12.97	87.03	0	12,97	87,03	0
Land Attack	-	-	-	-	-	-	0,58	99,42	0
SYN Flooding	0	13	87	26.71	0	73.29	2,27	97,73	0
HTTP	100	0	0	92.86	7.14	0	85,71	14,29	0
Telnet	100	0	0	100	0	0	100	0	0

Dari tabel terlihat bahwa k-nearest sudah bekerja dengan baik untuk hampir seluruh jenis serangan jika di bandingkan dengan metode yang lainya.hanya saja pada k-nn tidak mampu memproses

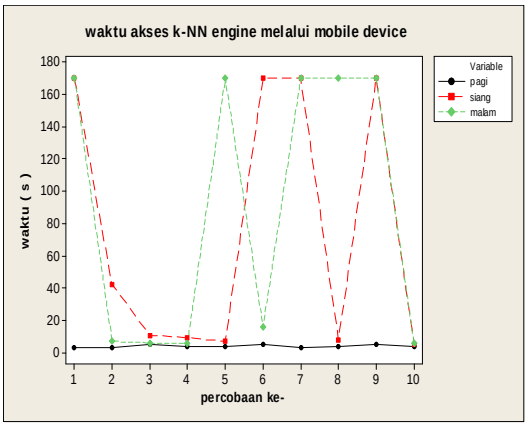
Tabel5.perbandingan waktu komputasi

Serangan	Hierarchical Clustering (s)	K-Nearest Neighbor (s)	Fuzzy Neural Network (s)
FIN Scan	1.18	5.174	1.286
XMAS Scan	2.22	4.011	0.309
NULL Scan	0.012	0.044	0.214
Ping of Death	0.83	0.421	0.446
SYN Flooding	0.91	5.451	0.220
HTTP	0.09	0.185	0.220
Telnet	0.09	0.153	0.220
Rata-tara	0.762	2.206	0.714

Untuk perbandingan waktu komputasi terlihat bahwa k-Nearest neighbor memiliki waktu komputasi rata-rata terlama yaitu 2.206s sedangkan waktu komputasi tercepat yaitu fuzzy neural network yaitu 0.714%

4.4 Percobaan akses HP

Percobaan ke-	Pagi (s)	Siang (s)	Malam (s)
1	3	170	170
2	3	42	6.97
3	5	10.69	5.92
4	4	9.37	5.91
5	4	6.8	170
6	5	170	15.73
7	3	170	170
8	4	7.92	170
9	5	170	170
10	4	5.07	6.04



jadi terlihat waktu pengaksesan yang paling baik adalah pagi hari yaitu sekitar 4s.

5. KESIMPULAN

1. kNN sudah baik untuk mendeteksi serangan sX yaitu 93.44% seranagan dan POD mendeteksi 100% serangan.
2. Jika dibandingkan dengan FUZZY maka semakin besar data base dan semakin kecil k maka persen bedanya semakin kecil.
3. Pada serangan Land_attack KNN belum mampu memprosesnya. terjadi error di sebabkan KNN waktu komputasi yang melebihi 30s dikarenakan jumlah packet data yang terlalu besar.
4. Jika dibandingkan dengan hierarchical clustering dan fuzzy neural network.k-Nearest neighbor sudah bekerja dengan baik hampir diseluruh serangan .namun mempunyai waktu komputasi terlama yaitu 2.206s
5. K-NN dapat di akses melalui aplikasi mobile dan waktu yang palib baik yaitu pagi hari dengan waktu rata-rata koneksi adalah 4s

6. DAFTAR PUSTAKA

[1] Bambang Wijanarko, "Algoritma Fuzzy Sebagai Metode Mendeteksi Pola Serangan Pada Jaringan Berbasis Snort IDS , Proyek Akhir PENS-ITS, 2009.

[2] Stephen Northcutt, Judy Novak, Network Intrusion Detection, New Riders, 2002.

[3] Stephen Northcutt, Judy Novak, Snort 2.1 Intrusion Detection,Paperback, 2006.

[4] Y.Liao and V.R.Vemuri, Use of K-Nearest Neighbor Classifier for Intrusion Detection, university of california,2002.

[5] M. Zen Somsono hadi,Modul Ajar Network Security, PENS-ITS,Surabaya, _ .

[6] Adebayo O. Adetunmbi, Samuel O. Falaki, Olumide S. Adewale and Boniface K. Alese, Network Intrusion Detection Based On Rugh Set and K-Nearest Neighbour, Department of Computer Science, Federal University of Technology, _ .