TRANSFORMTIKA, Vol.16, No.2, January 2019, pp. 190 - 195
ISSN: 1693-3656,
journals.usm.ac.id/index.php/transformatika ■page190

Sistem Deteksi Intrusi Jaringan pada Laboratorium Matematika Universitas Negeri Semarang

Dian Tri Wiyanti[1], David Mubarok[2], Wahyu Prasojo[3], Bihaqi Al Rafik[4]
[1]Program Studi Matematika FMIPA Universitas Negeri Semarang Semarang, Indonesia, e-mail:diantriwiyanti@mail.unnes.ac.id
[2]Program Studi Matematika FMIPA Universitas Negeri Semarang Semarang, Indonesia, e-mail:davidmubarok@mail.unnes.ac.id
[3]Program Studi Matematika FMIPA Universitas Negeri Semarang Semarang, Indonesia, e-mail:jojowahyu98@gmail.com
[4]Program Studi Matematika FMIPA Universitas Negeri Semarang Semarang, Indonesia, e-mail:bihaqialrafik@students.unnes.ac.id

ARTICLEI N F O

Article history:

Received 26 November 2018
Received in revised form 15 Desember 2018
Accepted 29 January 2019
Available online 31 Januari 2019

ABSTRACT

Increasingly rapid technological development is directly proportional to social interaction and has become a life style. The need for the internet and its various functions are increasingly popular in the community, because speed and convenience are increasingly needed. In the end, the internet was demanding quality network security also needs to be improved. On development, security is an important aspect of a system. The focus of this research is on Intrusion Detection System (IDS) or network intrusion system, which is an ability possessedbya system or device tobeable to detect attacks that might occur in the network. Internet activities and attacks on computer systems are increasing. This makes a very large data shouldbeanalyzed. Data Mining methods can be an option for detecting intrusion for problems with increasing large amounts of data. Issues toberesolved in this research is the detection of intrusionbycomparing network traffic patterns with patterns of known attacks (misuse), orbylooking for patterns of network traffic that is not normal (anomaly).

Keywords:Intrusion Detection System, Data Mining, C4.5 algorithm

1. Pendahuluan

Dunia berkembang sangat cepat sejalan dengan perkembangan teknologi. Hal ini pun berbanding lurus dengan interaksi sosial. Dewasa ini, teknologi dan sistem informasi menjadi*lifestyle*, dimana kepuasan*user*yang terletak pada kualitas pelayanan yang*cheaper*(lebih murah),*better*(lebih baik), dan*faster*(lebih cepat) semakin dicari. Kebutuhan akan internet dan beragam fungsinya kian digemari di masyarakat. Dikarenakan kecepatan dan kemudahannya semakin dicari, pada akhirnya internet pun menuntut kualitas keamanan jaringan yang juga perlu ditingkatkan.

Pada perkembangan teknologi komputer seperti internet sekarang, keamanan merupakan aspek penting dari suatu sistem. Saat ini hampir seluruh kalangan masyarakat dapat menggunakannya untuk mendapatkan informasi yang luas dan beragam dari seluruh dunia. Banyak kalangan seringkali tidak bertanggung jawab dalam menggunakan teknologi internet saat ini, yang sering kali menyebabkan kerugian. Hal ini pula yang menyebabkan munculnya serangan-serangan di dalam suatu jaringan komputer yang tentunya merugikan [1]. Terutama dengan semakin terbukanya pengetahuan*hacking*dan*cracking*, didukung dengan banyaknya*tools*yang tersedia dengan mudah dan gratis, semakin mempermudah para*intruder*dan*attacker*untuk melakukan aksi penyusupan ataupun serangan[2].

Fokus penelitian ini adalah mengenai*Intrusion Detection System*(IDS) atau sistem intrusi jaringan. IDS merupakan sebuah kemampuan yang dimiliki oleh sebuah sistem atau perangkat untuk dapat melakukan deteksi terhadap serangan yang mungkin terjadi dalam jaringan, baik lokal maupun yang terhubung dengan internet [3]. Pada umumnya, IDS dibagi menjadi dua bentuk yang digunakan saat ini, yaitu*Network-Based Intrusion DetectionS y s t e m*

Received November 26, 2018; Revised Desember 15, 2018; Accepted January 29, 2019

(NIDS) dan*Host-Based Intrusion Detection System*(HIDS). Keduanya memiliki perbedaan dalam mendeteksi dan menangguhkan serangan. Keduanya dapat dikembangkan, sehingga hasilnya lebih efektif mendeteksi setiap penyusupan dan menyiapkan strategi yang tepat [4].

Aktifitas internet dan serangan terhadap sistem komputer yang semakin meningkat, menyebabkan data yang harus dianalisis menjadi sangat besar. Hal ini selain menjadi masalah dan tantangan, namun juga menjadi sebuah kesempatan untuk penerapan sebuah metode pemilahan data dan membentuk skenario dari data yang banyak tersebut. Metode Data Mining dapat menjadi salah satu pilihan untuk mendeteksi intrusi dari permasalahan peningkatan jumlah data yang besar. Aplikasi-aplikasi dalam Data Mining dapat menemukan suatu pola yang rutin dalam suatu kumpulan data yang besar. Selain itu juga dapat memberikan solusi untuk masalah reduksi data pada kumpulan data tersebut sehingga memudahkan analis untuk melakukan identifikasi dan memberikan analisis data lebih efisien [5].

Tujuan dari penelitian ini adalah untuk mengklasifikasikan serangan pada data-data yang diujikan dengan menggunakan salah satu algoritma klasifikasi pada Data Mining. Algoritma C4.5, yang merupakan pengembangan dari algoritma ID3, adalah salah satu algoritma klasifikasi yang berfungsi untuk membuat*decision tree*(pohon keputusan).*Decision tree*berguna untuk mengekplorasi data dengan menemukan hubungan yang tersembunyi antara variabel input dengan variabel target. Data (input) pada algoritma C4.5 berupa tabel dan menghasilkan output berupa pohon [3]

2. Metode

a. Analisa Data yang digunakan

Tahap awal yang dilakukan adalah merekam lalu lintas paket data dalam jaringan komputer. Data tersebut digunakan untuk mendeteksi intrusi. Data akan direkam menggunakan aplikasi*network monitoring*, dalam bentuk*pcap files*. IDS mengumpulkan dan memonitor sistem operasi dan aktivitas data pada jaringan, juga menganalisis informasi untuk menjelaskan keadaan selama terjadinya penyerangan. IDS diklasifikasikan dalam 2 kategori berdasarkan bagaimana data dianalisis. Kategorinya adalah:

- *Misusedetection*
  Metode ini dilakukan dengan mencocokkan pola lalu lintas jaringan dengan pola serangan yang telah diketahui. Pola ini dipelajari dengan memeriksa seluruh data yang datang untuk menemukan tipe*intrusion*. Metode ini tidak mampu mendeteksi serangan baru yang polanya belum diketahui.
- *Anomalydetection*
  Pola dipelajari dari data normal. Data yang tidak terlihat dicek dan dicari penyimpangan dari pola yang telah dipelajari. Metode ini dilakukan dengan mencari pola lalu lintas jaringan yang tidak normal.

b. DataMining

Teknik data mining dapat diterapkan pada network based IDS untuk melindungi military subnetwork. Setiap military subnetwork adalah suatu pemeriksaan yang menyaring dan membukukan traffic network ke dalam database pusat. Sebuah rule set digunakan untuk menganalisis archived data untuk menemukan pola intrusive. Pola yang ditemukan terlihat sederhana, seperti melihat aktivitas yang berlebihansepertikoneksi dari IP address yang mempunyai kebiasaan intrusive. Contoh dari tipe intrusion seperti ini adalah serangan yang rendahdanlamayangberisikebiasaanintrusiveselamaberjam-jam,berhari-hariatauberminggu-mingguyangdimulaidariberbagaijaringan.Dataminingdapatditerapkanpadamasalahiniuntuk mengembangkan*human pattern recognition*. Tabel 4.1 berikut ini merupakan sebagian dataset dari trafik jaringan yang ada di laboratorium jurusan Matematika D10 lantai 3. Dataset diambil dengan aplikasi Wireshark, dengan jumlah data training sebanyak 450, dan data testing sejumlah 550.

Tabel 1. Dataset Trafik Jaringan

Time	Source	Destination	Protocol	Length
0	Routerbo_3b:03:f4	Broadcast	ARP	60
0,099966249	Routerbo_3b:03:f4	Broadcast	ARP	60
0,161840414	103.23.100.9	103.23.103.214	ICMP	98
0,240234723	Routerbo_3b:03:f4	Broadcast	ARP	60
0,249912229	Routerbo_3b:03:f4	Broadcast	ARP	60
0,352254444	Routerbo_3b:03:f4	Broadcast	ARP	60
0,569199369	146.185.222.30	103.23.103.216	TCP	60
0,569223839	103.23.103.216	146.185.222.30	TCP	54
0,679985172	Routerbo_3b:03:f4	Broadcast	ARP	60
0,756929781	Routerbo_3b:03:f4	Broadcast	ARP	60
0,812674826	146.185.222.30	103.23.103.216	TCP	60
0,85998525	Routerbo_3b:03:f4	Broadcast	ARP	60
0,859998229	Routerbo_3b:03:f4	Broadcast	ARP	60
0,86990584	Routerbo_3b:03:f4	Broadcast	ARP	60
0,889907009	Routerbo_3b:03:f4	Broadcast	ARP	60
0,919959332	Routerbo_3b:03:f4	Broadcast	ARP	60

c. Algoritma DecisionTree

Berikut langkah-langkah perhitungan manual dari algoritma Decision Tree untuk pemecahan masalah deteksi anomali trafik pada jaringan dengan menggunakan data training yang telah disiapkan sebelumnya.

Input : dataset*D*, output: decision tree*T*.

Langkah-langkah :

1) Siapkan datatraining.
2) Pilih atribut sebagaiakar

   Untuk memilih atribut akar, didasarkan pada nilai Gain tertinggi dari atribut-atribut yang ada.

   Untuk mendapatkan nilai Gain, harus ditentukan terlebih dahulu nilai Entropy.

   Rumus Entropy :

$$Entropy(S)=\sum_{i=1}^{n}-pi*\log_2 pi \quad (1)$$

   dengan :

   - *S* = Himpunan Kasus
   - *n* = Jumlah Partisi*S*
   - *pi* = Proporsi dari*Si*terhadap*S*

   Rumus Gain :

$$Gain(S,A)=Entropy(S)-\sum_{i=1}^{n}\frac{|S_i|}{|S|}*Entropy(S)_i \quad (2)$$

dengan :

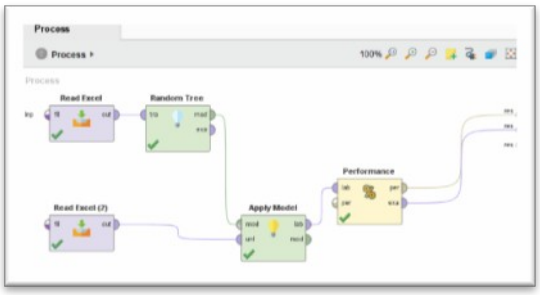
- *S* = Himpunan Kasus
- *A* =A t r i b u t
- *n* = Jumlah Partisi Atribut*A*
- | Si | = Jumlah Kasus pada partisi ke-*i*
- | S | = Jumlah Kasus dalam*S*

3) Buat cabang untuk tiap-tiapnilai.
4) Ulangi proses untuk setiap cabang sampai semua kasus pada cabang memiliki kelas yg sama. Ketika bentuk pohon keputusan selasai, maka algoritmaberakhir.

3. Hasil danPembahasan

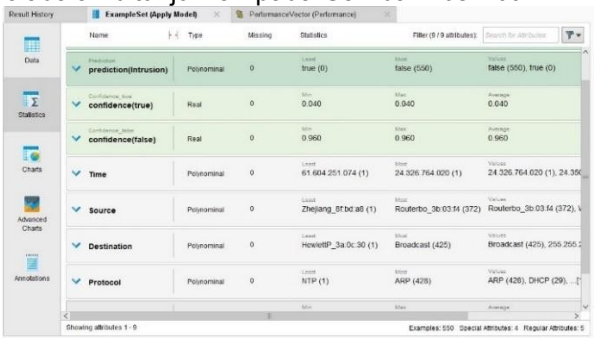
a. PenerapanDecision Tree dengan RapidminerStudio9.0

RapidMiner Studio menggabungkan teknologi dan penerapan untuk melayani integrasi yang*user friendly*. Menentukan proses analisis dengan RapidMiner Studio dilakukan dengan operator*drag and drop*, pengaturan parameter dan pengabungan operator. Dataset trafik dibagi 2, yaitu data training dan data testing. Dalam data training yang diproses, diperoleh model yang dapat diaplikasikan dalam data testing. Berikut gambaran proses yang dilakukan dengan RapidMiner:



Gambar 1. Proses Analisis Data Training dan Testing dengan Random Tree

Operator Random Tree mempelajari pohon keputusan. Operator ini hanya menggunakan subkumpulan atribut acak untuk setiap pemisahan, dan bekerja persis seperti operator Decision Tree dengan satu pengecualian, yaitu untuk setiap split hanya subset acak dari atribut tersedia. Operator ini belajar Decision Tree baik dari data nominal dan numerik. Atribut masukan untuk proses analisa adalah Time, Source, Destination, Protocol, dan Length. Sedangkan atribut keluarannya adalah Intrusion dengan hasil keputusan True atau False. True apabila diindikasikan terdapat*intrusion*atau gejala penyusupan, dan False jika tidak berindikasi adanya penyusupan ke dalam jaringan yang ada pada laboratorium jurusan Matematika D10.Setelah dilakukan proses analisa, hasil dari*apply model*adalah ditunjukkan pada Gambar 2berikut.

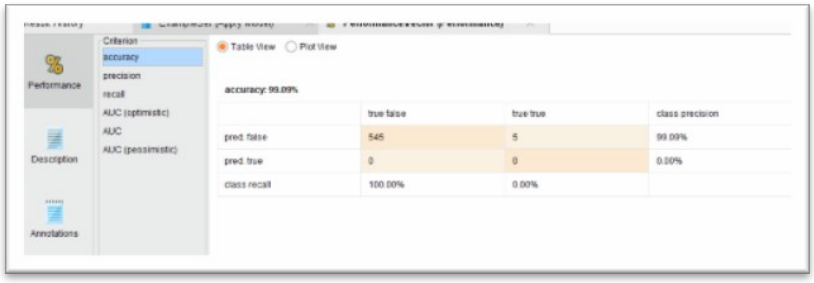


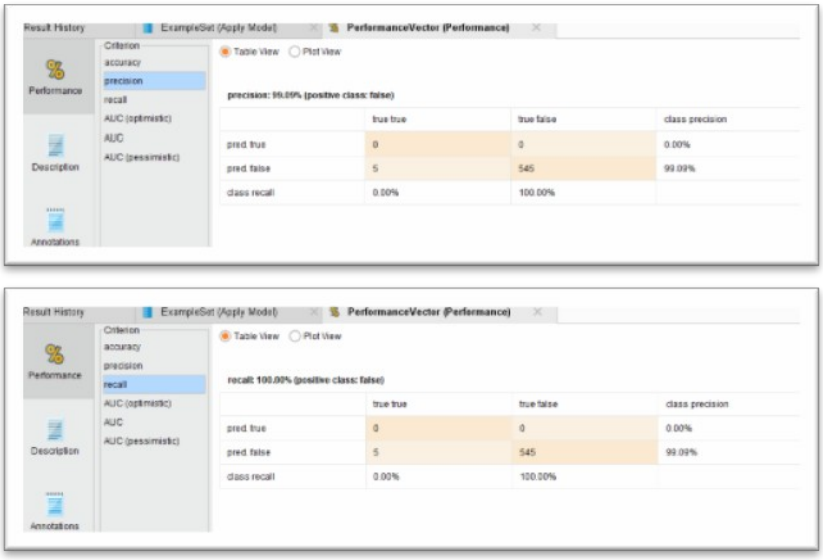
Gambar 2. Apply Model menggunakan Rapidminer

Hasil yangdapatdibacaadalah keseluruhan nilai darilabel Intrusion (keluaran),seharusnyabernilaiFalse.Artinya, dapatdikatakan bahwatrafik jaringan pada laboratorium jurusan Matematika D10 aman dari penyusup, dikarenakan tidak bahwa tidak ada kecenderungan Intrusion bernilai True dari dataset yang ada.

b. Performance

Berikutnya adalah pembacaan nilai performance dari dataset trafik jaringan.Operator Performance ini digunakan untuk evaluasi kinerja. Ini memberikan daftar nilai kriteria kinerja. Kriteria kinerja ini secara otomatis ditentukan agar sesuai dengan jenis*learning task*. Berbeda dengan operator evaluasi kinerja lainnya seperti operator Klasifikasi dan operator Regresi, operator Performance ini dapat digunakan untuk semua jenis tugas belajar, dan secara otomatis menentukan jenis tugas dan menghitung kriteria yang paling umum untuk jenis itu. Berikut adalah hasil performance dari kriteriaaccuracy, precision, dan recall yang ditunjukkan pada Gambar 3.





Gambar 3. Hasil Performance dengan Kriteria Accuracy, Precision, Recall

Mayoritas hasil analisa untuk atribut Intrusion bernilai False. Pengujian untuk Analisa tersebut dibuktikan dengan adanya nilai performance accuracy 99.09%, nilai precision 99.09% dengan positif adanya indikasi penyusupan adalah false. Dan dilanjutkan dengan nilai performance recall 100%, yang artinya menunjukkan bahwa keseluruhan dataset trafik jaringan cenderung aman dari penyusup.

4. Kesimpulan

Penelitian ini telah dilakukan dengan menggunakan model C4.5 untuk diimplementasikan pada sistem analisa data testing, sehingga dapat disimpulkan hasil dari percobaan antara lain:

1. Penelitian ini menggunakan metode klasifikasi dengan algoritma C4.5 untuk pembentukan rule, sebelum melakukan pemodelan C4.5 dilakukan preprocessing data menggunakan data training. Jumlah atribut masukan pada data penelitian ini yang berasal dari data trafik laboratorium jurusan Matematika D10 adalah 5 atribut, yaitu Time, Source, Destination, Protocol, dan Length. Sedangkan atribut keluaran adalah Intrusion.
2. Nilai performance akurasi 99.09%, nilai precision 99.09% dengan positif adanya indikasi penyusupan adalah false, dan recall 100%.
3. Sistem yang dibuat hanya untuk pengujian data testing dan menampilkan data hasil aplikasi model danperformance.

References

[1] J. R. Ramadhani, Y. Purwanto and T. W. Purboyo, "Analisis Metode Covariance Matrix Menggunakan Teknik Landmark Window Untuk Sistem Deteksi Anomali Trafik," in *e-Proceeding of Engineering*, 2015.

[2] S. A. Budiman, C. Iswahyudi and M. Sholeh, "Implementasi Intrussion Detection System (IDS) Dengan Menggunakan Jejaring Sosial Sebagai Media Notifikasi," in *Prosiding SeminarNasional Aplikasi Sains & Teknologi (SNAST)*, Yogyakarta, 2014 .

[3] I. Khaerani and L. B. Handoko, "Implementasi dan Analisa Hasil Data Mining untuk Klasifikasi Serangan pada Intrusion Detection System (IDS) dengan Algoritma C4.5,"*Techno.COM,*pp. 181-188,2015.

[4] T. Thomas, Network Security First-Step, Yogyakarta: Penerbit Andi, 2005.

[5] A. Agathou and T. Tzouramanis, The Role Of Data mining in Intrusion Detection Technology, New York: Garson, G.D. dan Khosrow-Pour,M (ed.), Handbook of Research on Public

Information Technology, Vol.1, Information Science Reference, 2008.

[6] I. W. O. K. Putra, Y. Purwanto and F. Y. Suratman, "Perancangan dan Analisis Deteksi Anomali Berbasis Clustering Menggunakan Algoritma Modified K-Means dengan Timestamp Initialization pada Sliding Window," in*e-Proceeding of Engineering*, 2015.

[7] A. Jacobus and E. Winarko, "Penerapan Metode Support Vector Machine pada Sistem Deteksi Intrusi secara Real-time,"*Berkala MIPA ,*pp. 172-185, 2013.

[8] D. Ariyus, Intrusion Detection System, Andi, Yogyakarta: Penerbit Andi, 2007.

[9] J. Han and M. Kamber, Data mining: Concepts and Techniques, San Francisco, USA: Morgan Kaufmann Publishers, 2006.

[10] W. Lee, "A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems," Tesis, School of Arts and Sciences Columbia University, New York, 1999.