ANALISA SERANGAN SMURF DAN PING OF DEATH DENGAN METODE SUPPORT VECTOR MACHINE (SVM)

Henni Endah Wahanani[1], Budi Nugroho[2], Galih Indo Prakoso[3]
[123]Program Studi Teknik Informatika, Fakultas Teknologi Industri, UPN "Veteran" Jawa Timur, Surabaya
henniendah222@gmail.com[1], budinug@gmail.com[2]

Abstrak. *Serangan atau intrusi sangat tidak diinginkan pada sistem jaringan komputer karena bisa membahayakan integritas, kerahasiaan dan ketersediaan sumber daya yang ada. Serangan DoS jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut. Masalah datang dimulai ketika paket data yang datang sangat banyak dan harus dianalisa di kemudian hari. Teknik data mining merupakan teknik yang tepat untuk melakukan analisa terhadap sebuah data.Pada penelitian ini akan melakukan klasifikasi serangan pada data-data yang diuji dengan menggunakan metode klasifikasi SVM (Support Vector Machines). Data yang diklasifikasi dari serangan DoS yaitu Smurf, Ping of Death (PoD) dan Normal dengan mencatat aktivitas data traffic jaringan menggunakan tools TCPdump, selanjutnya menemukan informasi fitur yang relevan yang ada didalamnya dan menggunakan fitur tersebut untuk melakukan klasifikasi jenis intrusi dengan dataset KDD Cup DARPA 1999. Hasil penelitian ini Klasifikasi serangan dengan metode SVM menghasilkan tingkat akurasi yang cukup tinggi untuk masing-masing serangan dengan rata-rata class yang diprediksi di atas 60%.*

Kata kunci: Klasifikasi, SVM, Smurf, Ping of Death.

Jaringan komputer sekarang merupakan bagian dari dunia modernisasi komputer dan digunakan untuk hampir setiap bidang seperti berita, email, audio dan komunikasi video, *e-commerce*, sharing data dan banyak aplikasi lainnya sehingga keamanan jaringan komputer merupakan aspek yang sangat penting. Keamanan komputer tidak bisa dipisahkan dengan *firewall* dan *Intrusion Detection Sytem* (IDS). Bisa dikatakan kedua komponen ini wajib untuk dijalankan di semua jaringan. Jika *firewall* lebih kepada benteng penjaga, maka IDS adalah petugas pengawas sistem.

Beberapa serangan atau intrusi yang tidak diinginkan sering dilakukan pada sistem ini, untuk mengakses data penting. Sebuah intrusi atau dapat didefinisikan [1] sebagai "sekelompok peristiwa yang berbahaya untuk kerja yang aman dari sistem ". Intrusi bisa didefinisikan sebagai usaha yang bisa membahayakan integritas, kerahasiaan dan ketersediaan sumber daya yang ada [3][4]. Metode yang banyak dimanfaatkan untuk IDS dapat dikategorikan menjadi dua *Misuse detection* mendeteksi intrusi dengan mencocokkan pola lalu lintas jaringan dengan pola serangan telah diketahui (*misuse*). Metode yang kedua adalah *anomaly detection* sistem mendefinisikan pola atau behaviour jaringan sebelumnya. Semua deviasi dari pola normal akan dilaporkan sebagai serangan. Keuntungan utama dari *anomaly* adalah kemampuan untuk mendeteksi serangan yang sebelumnya belum didefinisikan. DoS (*Denial of Service*) merupakan serangan yang berbasis *anomaly*.

Serangan DoS adalah jenis serangan terhadap sebuah komputer atau *server* di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Masalah dimulai ketika paket data yang datang sangat banyak dan harus di analisa di kemudian hari. Teknik Data Mining merupakan teknik yang tepat untuk melakukan analisa terhadap sebuah data. Beberapa penelitian telah menggunakan teknik data mining untuk mengatasi masalah serangan IDS seperti analisis *frequent* itemset, analisis *clustering*, analisis klasifikasi dan analisis asosiasi. Tujuan dari penelitian ini adalah untuk mengklasifikasikan serangan pada data-data yang diujikan dengan

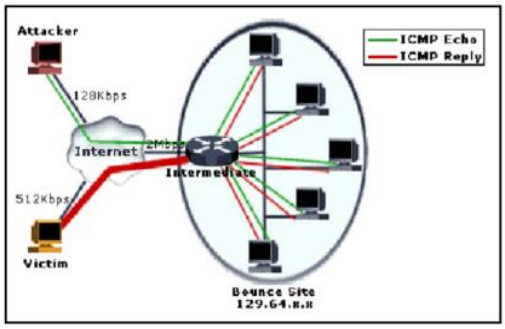
menggunakan metode klasifikasi yaitu *Support Vector Machines* (SVM).

Penelitian ini dititikberatkan pada serangan *Smurf* dan *Ping of Death* (PoD) dengan mencatat aktivitas data traffic jaringan menggunakan *tools* tcpdump, selanjutnya menemukan informasi fitur yang relevan yang ada didalamnya dan menggunakan fitur tersebut untuk melakukan klasifikasi jenis intrusi yaitu menggunakan metode SVM dengan dataset KDD Cup DARPA 1999.

I. Metodologi

Ping of Death

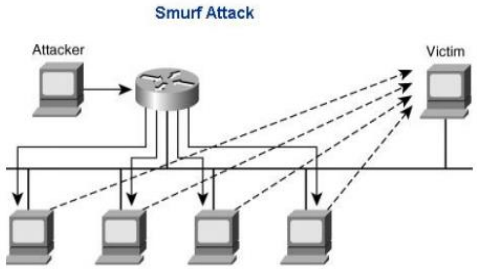
Ping of Death adalah serangan *Denial of Service* yang disebabkan oleh penyerang. Penyerang dapat mengirim paket IP lebih dari 65.536 byte, yang diijinkan oleh protokol IP. Ini adalah salah satu fitur protokol TCP / IP dengan memecah-belah paket yang masuk menjadi sub paket [5] [6]. Protokol IP memungkinkan satu paket dan dipecah menjadi paket-paket kecil. Jenis serangan ini menggunakan *utility ping* yang ada pada sistem operasi komputer. *Ping* ini digunakan untuk mengecek waktu yang akan diperlukan untuk mengirim data tertentu dari satu komputer ke komputer lainnya.



Gambar 1. *Ping of Death* [7]

Smurf

Smurf adalah serangan DoS yang memanfaatkan protokol internet. Intruder (penyusup) menggunakan fitur pada program *Smurf* yang menyebabkan jaringan bisa dioperasikan atau dikendalikan. Serangan *Smurf* mengambil keuntungan tertentu atas protokol internet (IP) dan ICMP dengan menggunakan karakteristik protokol ini melalui internet [6]. Pada Gambar 2. terlihat bahwa ICMP digunakan oleh komponen jaringan dan administrator untuk mengirim pesan pemberitahuan *error* antara *node* ke *server*.



Gambar 2. *Smurf* [9]

Alamat IP tujuan pada paket yang dikirim adalah alamat *broadcast* dari jaringan, maka *router* akan mengirimkan permintaan *ICMP echo* ini ke semua mesin yang ada di jaringan. Kalau ada banyak *host* di jaringan, maka akan terjadi trafik *ICMP echo* respons & permintaan dalam jumlah yang sangat besar. Akibat serangan *Smurf attack* ini adalah jika *hacker* ini memilih untuk men-*spoof* alamat IP sumber permintaan ICMP tersebut, akibatnya ICMP trafik tidak hanya akan membuat macet jaringan komputer perantara saja, tapi jaringan yang alamat IP-nya di *spoof* jaringan ini di kenal sebagai jaringan korban (*victim*)[8][9].

Klasifikasi

Klasifikasi dan prediksi adalah dua bentuk analisis data yang bisa digunakan untuk mengekstrak model dari data yang berisi kelas-kelas atau untuk memprediksi trend data yang akan datang. Klasifikasi memprediksi data dalam bentuk kategori, sedangkan prediksi memodelkan fungsi-fungsi dari nilai yang kontinyu. Misalnya model klasifikasi bisa dibuat untuk mengelompokkan aplikasi peminjaman pada bank apakah beresiko atau aman, sedangkan model prediksi bisa dibuat untuk memprediksi pengeluaran untuk membeli peralatan komputer dari pelanggan potensial berdasarkan pendapatan dan lokasi tinggalnya. Prediksi bisa dipandang sebagai pembentukan dan penggunaan model untuk menguji kelas dari sampel yang tidak berlabel, atau menguji nilai atau rentang nilai dari suatu atribut[13].

Data input untuk klasifikasi adalah koleksi dari *record*. Setiap *record* dikenal sebagai *instance* atau contoh, yang ditentukan oleh sebuah tuple (x,y), dimana x adalah himpunan atribut dan y adalah atribut tertentu, yang dinyatakan sebagai label kelas. Pemodelan klasifikasi dibagi menjadi 2 yaitu pemodelan deskriptif dan pemodelan prediktif. Pemodelan deskriptif merupakan model klasifikasi dapat bertindak sebagai alat penjelas untuk membedakan objek-objek dari kelas-kelas yang berbeda. Sedangkan pada pemodelan prediktif, model klasifikasi yang juga dapat digunakan untuk memprediksi label kelas dari *record* yang tidak diketahui. Beberapa teknik klasifikasi yang digunakan untuk jenis model ini adalah *support vector machine*, *rule-based classifier*, *decision tree classifier*, *neural network* dan *naive bayes classifier*

Pendekatan umum yang digunakan dalam masalah klasifikasi adalah pertama training set berisi *record* yang mempunyai label kelas yang diketahui haruslah tersedia. Training set digunakan untuk membangun model klasifikasi, yang kemudian diaplikasikan ke test set, yang berisi *record-record* dengan label kelas yang tidak diketahui.

SVM (Support Vector Machines)

Support Vector Machine dikembangkan oleh Boser, Guyon, Vapnik, dan pertama kali dipresentasikan pada tahun 1992 di *Annual Workshop on Computational Learning Theory*. Konsep SVM dapat dijelaskan secara sederhana sebagai usaha mencari *hyperplane* terbaik yang berfungsi sebagai pemisah dua buah kelas pada input space. pattern yang merupakan anggota dari dua buah kelas : +1 dan -1 dan berbagi *alternative* garis pemisah (*discrimination boundaries*). Margin adalah jarak antara hyperplane tersebut dengan *pattern* terdekat dari masing-masing kelas. *Pattern* yang paling dekat ini disebut sebagai *support vector*. Usaha untuk mencari lokasi *hyperplane* ini merupakan inti dari proses pembelajaran pada SVM[10].

Pembahasan teori SVM dimulai dengan kasus klasifikasi yang secara linier bisa dipisahkan. Dalam hal ini fungsi pemisah yang dicari adalah fungsi linier. Fungsi ini bisa didefinisikan sebagai

g(x) := sgn(f(x))

dengan $f(x)=w^{\mathrm{T}}x+b$

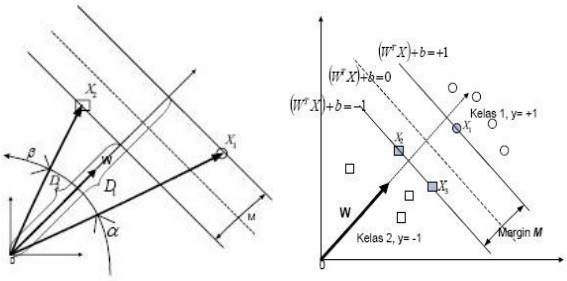
$$atau\ g(x) = \begin{cases} +1, jika\ (Wx+b) \geq +1 \\ -1, jika\ (Wx+b) \leq -1 \end{cases}$$

dimana $x, w \in \Re^n$ and $b \in \Re$. Masalah klasifikasi ini bisa dirumuskan sebagai berikut: kita ingin menemukan set parameter (w, b) sehingga $f(xi) =< w, x > +b = yi$ untuk semua i. Dalam teknik ini kita berusaha menemukan fungsi pemisah (*klasifier/hyperplane*) terbaik diantara fungsi yang tidak terbatas jumlahnya untuk memisahkan dua macam obyek.

Hyperplane terbaik adalah *hyperplane* yang terletak di tengah-tengah antara dua set obyek dari dua kelas. Mencari *hyperplane* terbaik ekuivalen dengan memaksimalkan margin atau jarak antara dua set obyek dari kelas yang berbeda. Jika $wx_1+b=+1$ adalah pendukung *hyperplane* dari kelas +1 ($wx_2+b=+1$) dan $wx_2+b=-1$ pendukung *hyperplane* dari kelas $-1(wx_2+b=-1)$, margin antara dua kelas dapat dihitung dengan mencari jarak antara kedua pendukung hyperplane dari kedua kelas. Secara spesifik, margin dihitung dengan cara berikut:

$$w(x_1 - x_2)) = 2 \rightarrow \left(\frac{w}{||w||}(x_1 - x_2)\right) = \frac{2}{||w||}$$

Dan secara detailnya bagaimana nilai margin optimal diperoleh seperti dijelaskan pada gambar 3 berikut ini :



(a) (b)

Gambar 3.(a). Nilai jarak optimal (b) hyperplane

Confusion Matrix

Confusion matrix merupakan metode yang menggunakan tabel matriks seperti pada Tabel 1, jika data set hanya terdiri dari dua kelas, kelas yang satu dianggap sebagai positif dan yang lainnya negatif [11]

Tabel 1. Model Confusion Matrix

		True Class	
		Positive	*Negative*
Predicted Class	*Positive*	*True positives count (TP)*	*False negatives count (FP)*
	Negative	*False positives count (FN)*	*True negatives count (TN)*

True positives adalah jumlah *record* positif yang diklasifikasikan sebagai positif, *false positives* adalah jumlah *record* negatif yang diklasifikasikan sebagai positif, *false negatives* adalah jumlah *record* positif yang diklasifikasikan sebagai negatif, *true negatives* adalah jumlah *record* negatif yang diklasifikasikan sebagai *negative*, kemudian masukkan data uji. Setelah data-data telah masuk ke dalam confusion matrix maka dapat dihitung nilai-nilai sensitivity (*recall*), *specificity*, *precision* dan *accuracy*. Untuk menghitung digunakan persamaan di bawah ini[11]:

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP}$$

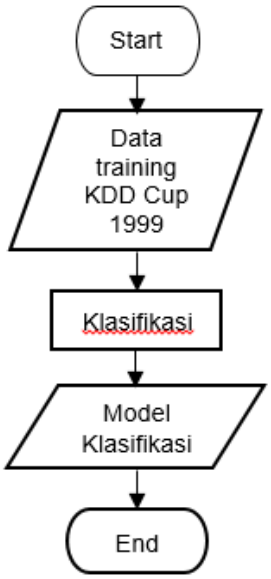
ROC Curve

ROC (*Receiver Operating Characteristics*) *curve* adalah pengujian berdasarkan performanya. ROC mengekspresikan *confusion matrix*. Nilai dari ROC *curve* hanya terdiri dari 0 sampai 1. Semakin nilai ROC *curve* mendekati 1 maka akan semakin baik seperti diperlihatkan pada Tabel 2.

Tabel 2. Klasifikasi Akurasi [12]

0,90 – 1,00	Excellent Classification
0,80 – 0,90	Good Classification
0,70 – 0,08	Fair Classification
0,60 – 0,70	Poor Classification
0,50 – 0,60	Failure

Mekanisme Pembentukan Model Klasifikasi



Gambar 4. Pembentukan Model Klasifikasi

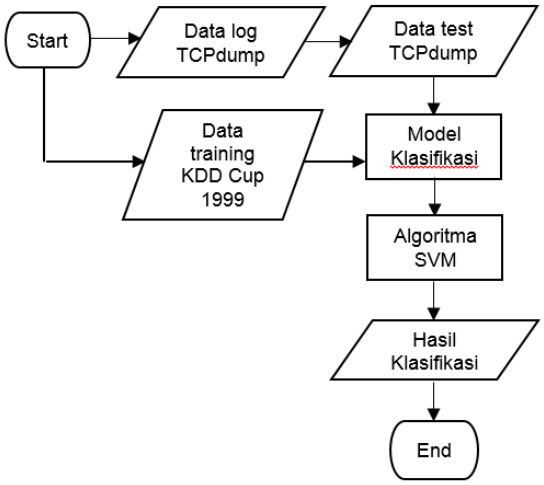
Pada Gambar 4., *dataset* KDD CUP 1999 digunakan sebagai *data training* untuk membentuk sebuah model klasifikasi. *Data training* tersebut akan di klasifikasi dengan menggunakan RAPIDMINER. Dalam proses klasifikasi nantinya akan menggunakan salah satu algoritma yang terdapat pada RAPIDMINER yaitu algoritma SVM. Hasil dari klasifikasi data training tersebut akan membentuk sebuah model klasifikasi yang akan digunakan dalam mengklasifikasi *data test*.

Mekanisme Klasifikasi

Pada Gambar 5. mekanisme klasifikasi data log mentah TCPdump yang berisi paket-paket serangan *Smurf, Ping of Death* dan normal yang nantinya akan dicapture oleh wireshark (trafik jaringan) untuk mendapatkan protokol jaringan yang akan diolah sesuai atribut yang telah ditentukan, setelah data diperoleh maka akan disimpan di dalam database microsoft excel yang kemudian dikonversi menjadi sebuah dataset yang akan digunakan untuk klasifikasi serangan.

Dalam proses klasifikasi, dataset KDD CUP 1999 akan digunakan sebagai data training untuk membentuk sebuah model klasifikasi dimana akan dilakukan pengujian terhadap model tersebut menggunakan data test serangan *Smurf,*

Ping of Death dan normal dengan menggunakan perangkat lunak RAPIDMINER untuk mengetahui hasil klasifikasi serangan terhadap dataset yang dibuat.

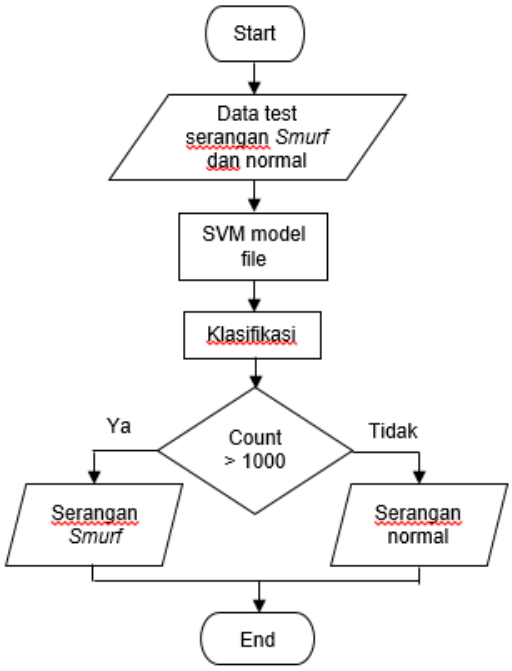


Gambar 5. Klasifikasi DoS

Mekanisme Serangan

Didalam mekanisme serangan ini akan dilakukan klasifikasi terhadap data test TCPdump menggunakan 3 serangan yaitu *Ping of Death*, *Smurf* dan Normal. setiap dataset serangan berisi masing-masing 500 *record* data, jadi total data yang dibuat dengan 3 serangan ini sekitar 1500 *record* data serangan.

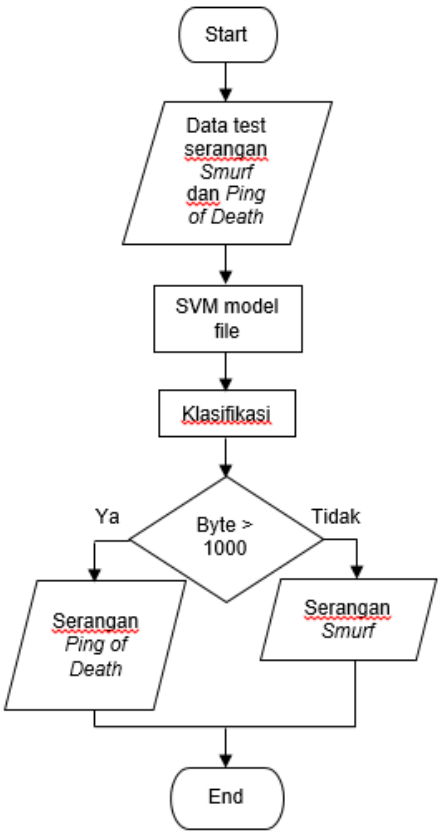
Serangan *Smurf* dan Normal



Gambar 6. Mekanisme Serangan *Smurf* dan Normal

Pada Gambar 6. data test berisikan paket-paket serangan *Smurf* dan Normal setelah itu dilakukan accuracy dari algoritma SVM untuk membedakan antara 2 serangan yang dipilih yaitu serangan *Smurf* dan Normal. Hal ini bisa dilihat melalui paket yang masuk disetiap 2 detiknya. Jika paket serangan yang masuk di setiap 2 detiknya lebih dari 1000 paket berarti di anggap serangan *Smurf* dan lebih kecil dianggap serangan Normal.

Serangan *Smurf* dan *Ping of Death*



Gambar 7. Mekanisme serangan *Smurf* dan *Ping of Death*

Pada Gambar 7. data test berisikan paket-paket serangan *Smurf* dan *Ping of Death* setelah itu dilakukan *accuracy* dari algoritma SVM untuk membedakan antara 2 serangan yang dipilih yaitu serangan *Smurf* dan *Ping of Death*. Hal ini bisa dilihat melalui paket yang masuk disetiap 2 detiknya. Jika paket serangan yang masuk di setiap 2 detiknya lebih dari 1000 paket berarti di anggap serangan *Ping of Death* dan lebih kecil dianggap serangan *Smurf*.

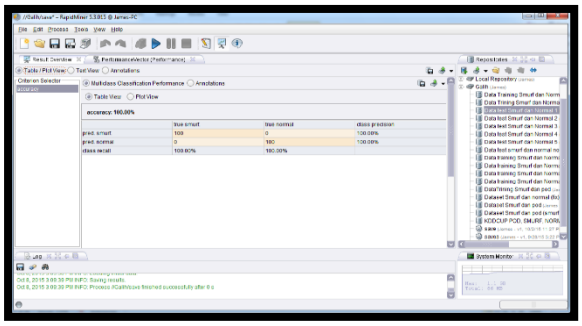
II. Hasil Dan Pembahasan

Penelitian ini menggunakan data log mentah dari TCPdump untuk menangkap paket-paket serangan Smurf, Ping of Death dan Normal yang ada di jaringan dan hasilnya akan diproses untuk pembuatan dataset, dimana hasil capturing dari data log mentah tadi menggunakan perangkat lunak Wireshark untuk mendapat nilai dari atribut-atribut yang akan digunakan. Setelah melakukan pengolahan data log TCPdump dan mendapat nilai dari masing-masing atribut maka data tersebut disimpan ke database menggunakan Microsoft Office Excel dengan format *csv.

Database masing-masing serangan sebanyak 500 *record*. Setelah database selesai dibuat maka dilakukan import data pada RapidMiner. Selanjutnya dibuatan model klasifikasi berdasarkan data training KDD CUP 1999 yang berisikan 2 model klasifikasi yaitu *Smurf* dengan Normal dan *Smurf* dengan *Ping of Death*. Kemudian dilakukan klasifikasi pembuatan sebuah model yang dihasilkan dengan metode SVM. Pada penelitian ini dilakukan 5 kali percobaan dengan menggunakan 5 data test berbeda yang terdiri dari setiap satu dataset berisi serangan *Smurf* dan Normal begitu juga untuk serangan *Smurf* dan *Ping of Death*.

Hasil Uji Coba Serangan dengan SVM

Pada uji coba serangan dengan SVM akan menjelaskan tentang hasil yang ditunjukkan pada hasil klasifikasi data test, data yang digunakan terdiri dari 500 datatest serangan *Smurf*, 500 datatest *Ping of Death* dan 500 data test normal yang terlihat pada Gambar 8 dan Gambar 9. Tingkat akurasi dengan menggunakan algoritma SVM dalam mengklasifikasikan serangan terhadap data test yang dibuat rata-rata dari serangan *Smurf* dan normal yaitu sebesar 92,40%. Algoritma SVM disini bukan hanya menghitung tingkat akurasi tetapi juga dapat menghitung true *Smurf*, true normal, true *Ping of Death*, prediksi *Smurf*, prediksi *Ping of Death* dan prediksi normal. Berikut ini perhitungannya bisa dilihat pada tabel 3 dan tabel 4.

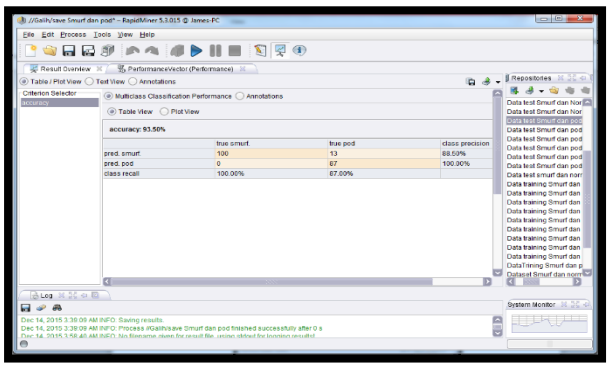


Gambar 9. Hasil evaluasi data test SVM serangan *Smurf* dan Normal

Tabel 3. Confusion Matrix Metode SVM serangan *Smurf* dan Normal

Accuracy : 92.40%			
	True *Smurf*	True Normal	*Class Precission*
Pred. *Smurf*	490	66	88.34%
Pred. Normal	10	434	100.00%
Class Recall	98.00%	86.80%	

Sedangkan tingkat akurasi dengan SVM rata-rata hasil dari klasifikasi serangan *Smurf* dan *Ping of Death* adalah sebesar 84,90%.



Gambar 10. Hasil evaluasi data test SVM serangan *Smurf* dan *Ping of Death*

Tabel 4. Confusion Matrix Metode SVM serangan *Smurf* dan *Ping of Death* (PoD)

Accuracy : 84.90%			
	True *Smurf*	True PoD	*Class Precission*
Pred. *Smurf*	490	141	78.00%
Pred. PoD	10	359	100.00%
Class Recall	98.00%	71.80%	

III. Simpulan

Klasifikasi serangan dengan metode SVM menghasilkan tingkat akurasi yang cukup tinggi untuk masing-masing serangan dengan rata-rata class yang diprediksi di atas 60%. Secara keseluruhan metode SVM terbukti cukup akurat dalam mengklasifikasikan serangan DoS yaitu serangan Smurf dan Normal yaitu hasil dari klasifikasi semua data test sebesar 92,4% dan terbukti juga cukup akurat dalam mengklasifikasikan serangan Smurf dan Ping of Death rata-rata keseluruhan hasil dari klasifikasi semua data test sebesar 84,9%

IV. Daftar Pustaka

[1] W. Lee and S. J. Stolfo, 1998, Data mining approaches for intrusion detection, at USENIX Security Symposium

[2] Damiano Bolzoni and Sandro Etalle, 2008, Approaches in Anomaly-based Network Intrusion Detection Systems.

[3] Like Zhang, Gregory B.White, 2007, Analysis of Payload Based Application Level Network Anomaly Detection, The 40th Hawaii International Conference on System Sciences.

[4] Qinglei Zhang, Wenying Feng, 2009. Network Intrusion Detection by Support Vectors and Ant Colony. Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009), pp 639-642.

[5] Ajey, Singh, Dr. Maneesh Shrivastana, 2012, Overview of Attacks on Cloud Computing, volume 1, issue 4.

[6] Vikas Chouhan and Sateesh Kumar, 2012, Packet Monitoring Approach to Prevent DDOS Attack in Cloud Computing, ISSN no. 2315-4209, vol.1

[7] Anonim, 2013, DOS Attack id.wikipedia.com.

[8] K. Thirupathi Rao *et al.*,2010, High Level Architecture to Provide Cloud Services Using Green Data Center, in Advances in Wireless and Mobile Communications (AWMC) *Volume 3 Number 2, pp 109-119*, Research India Publication ISSN 0973-697

[9] T.Gunasekhar, K.Thirupathi Rao, P.Saikiran, P.V.S Lakshmi, 2014, A Survey on *Denial of Service* Attack, International Journal of Computer Science

[10] and Information Technologies (IJCSIT), Vol. 5

[11] Cristianini, Nello and John Shawe-Taylor. , 2000. An Introduction to Support Vector Machines. Cambridge University Press, Cambridge, UK

[12] Olson, David and Yong, Shi. 2008. Pengantar Ilmu Penggalian Data Bisnis (Criswan Sungkono Penerjemah). Jakarta: Salemba Empat,.

[13] Gorunescu, Florin. 2011. Data Mining Concepts, Model and Techniques. s.l. : Springer.

[14] Han J, Kamber M. 2006. Data Mining:Concepts and Techniques. San Francisco: Morgan Kaufmann Publisher.

Halaman ini sengaja dikosongkan.