LOFIAN: Jurna**l** Tekn**o**logi In**f**ormas**i** d**a**n Komu**n**ikasi
https://ejournal.umbp.ac.id/index.php/lofian/
Vol. 5, No. 1, Agustus 2025, Halaman 13-19

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Implementasi Algoritma Principal Component Analisys dan Jaringan Syaraf Tiruan Dalam Mengoptimasi Fitur dan Performa Intrusion Detection System

Fauzi Haris Simbolon[1], Sartana[2], Maranata Pasaribu[3], Marice Hotnauli Simbolon[4], Maradu Sihombing[5]

[1,2,3,4,5]*Universitas Mandiri Bina Prestasi*
Jl. Letjend. Djamin Ginting No. 285-287, Padang Bulan, Medan Baru, Kota Medan, Sumatera Utara, Indonesia - 20155

[1]*farizboy@gmail.com*, [2]*sartanasinurat@gmail.com*, [3]*kiainggo@gmail.com*, [4]*simbolonice@gmail.com*, [5]*maradus71@gmail.com*

DOI: https://doi.org/10.58918/yyzrza47

Abstrak

Mengamankan data dan informasi merupakan aktivitas yang sangat dibutuhkan dalam dunia idustri, bisnis maupun perkantoran terutama terkait dengan data dan informasi yang dikirim melalui jaringan. Intrusion Detection System atau Sistem deteksi intrusi (IDS) merupakan suatu produk perangkat keras atau perangkat lunak yang mampu mendeteksi aktivitas yang janggal, aneh dan mengandung unsur bahaya di jaringan komputer atau di host yang terpisah. IDS hanya memantau lalu lintas yang disalin, dan memberi peringatan, bahwa paket yang sebenarnya bermasalah telah terkirim ke target yang dituju. Bahkan jika telah dilakukan pengaturan IDS untuk memperbarui firewall dengan aturan pemblokiran, paket serangan awal sudah terlanjur masuk Pelaksanaan proses intrusi berkecepatan tinggi tentunya akan menimbulkan beberapa kendala yang cukup signifikan terutama masalah dimensionalitas yang sangat besar, untuk itu dibutuhkan algoritma Principal Component Analisys (PCA) untuk menangani masalah tersebut, dengan algoritma ini memungkinkan peningkatan kinerja pengklasifikasian Jaringan Syaraf Tiruan (JST) dalam deteksi intrusi. Melalui bantuan algoritma PCA dapat diidentifikasi 15 fitur teratas dari 41 fitur yang terdapat pada kumpulan fitur KDD Cup 1999, dan perolehan peningkatan lebih dari 62% pada saat pelatihan JST. melalui pengujian menggunakan JST dapat disimpulkan bawa Jaringan Saraf Tiruan Multi Layer Perceptron dapat meningkatkan akurasi bahkan setelah mereduksi fitur-fitur yang ada.

Kata Kunci: Fitur dan Performa, IDS, MLP, PCA, JST.

1. Pendahuluan

Deteksi serangan dalam jaringan komputer selalu menjadi tantangan yang dihadapi oleh administrator dan personel keamanan jaringan. Sistem Deteksi Intrusi (IDS) merupakan pilihan utama dan salah satu alat untuk keamanan trafik jaringan. Di antara dua jenis utama IDS, yaitu berbasis Penyalahgunaan (Misuse) dan berbasis Kejanggalan (Anomali), IDS berbasis Anomali memiliki keunggulan dibandingkan jenis lainnya dalam mendeteksi pola serangan yang baru dan terus berubah [7]. Banyak literatur dan penelitian yang membahas penggunaan Jaringan Syaraf Tiruan (JST) [12], [13], [6], [2] karena beberapa keunggulan seperti kemampuan belajar yang baik, adaptabilitas, toleran terhadap kesalahan, kemampuan implementasi perangkat keras, fitur inheren pemrosesan informasi kontekstual, konsumsi energi yang rendah dll. Dalam makalah ini, kami telah mengusulkan pengklasifikasi 15 kelas. Sebagian besar literatur didasarkan pada standar data evaluasi IDS KDD 1999 yang terdiri dari 41 fitur. Dalam studi ini, peeliti telah melatih dan menguji JST dengan seluruh 41 fitur dan juga mencoba mengoptimalkan set fitur dengan mengurangi jumlah fitur menjadi 15 menggunakan Principal Componenet Analisys (PCA). Pelatihan dan pengujian lebih lanjut menunjukkan peningkatan waktu pelatihan yang signifikan sebesar 62%.

J.P Anderson [3] mendefinisikan upaya intrusi dalam dan menciptakan ruang untuk beberapa studi dan teknik tentang IDS. Dorothy Denning [10] telah menginspirasi banyak peneliti dengan mengusulkan model Deteksi Intrusi berbasis anomali. Karya menarik dari Varun Chandola dkk [8], membahas berbagai mekanisme deteksi intrusi anomali. Karya serupa yang dilakukan oleh Fariba Haddadi dkk [4], menunjukkan pengklasifikasi lima kelas untuk mendeteksi intrusi dari kumpulan data DARPA yang melaporkan rata-rata tingkat deteksi 82,44%. Dalam karya lain [9], pengklasifikasi dua kelas berdasarkan jaringan saraf tiruan umpan-maju diusulkan. Jaringan

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Saraf Tiruan terbukti baik untuk deteksi anomali guna menemukan perilaku pengguna dalam [15]. Dalam [3], sistem deteksi intrusi Hibrida didemonstrasikan. Penggunaan PCA dalam [10] oleh Solomon Raju dkk. mereduksi kumpulan data kompleks menjadi dimensi untuk mengungkap struktur tersembunyi yang lebih rendah.

Dalam makalah oleh T. Petreus dkk. [5], PCA digunakan untuk mengekstraksi fitur-fitur penting dalam bidang bioinformatika. Dalam sebuah studi [6], peneliti menggunakan PCA untuk mendeteksi fitur perangkat lunak tersembunyi untuk analisis malware. Dalam [7], Leila Mechtri dkk. menggunakan PCA dan jaringan saraf abu-abu untuk klasifikasi data intrusi dengan lima kelas. Dalam penelitian saat ini, peneliti telah mengusulkan model pengklasifikasi multikelas baru yang dapat mendeteksi 15 kelas serangan termasuk trafik jaringan normal. Fitur-fitur yang dioptimalkan terbukti meningkatkan kinerja pada JST dengan mengurangi waktu pelatihan dan juga akurasi deteksi.

Adapun tujuan dari aktivitas penelitian ini adalah mengoptimasi fitur dan performa kinerja Sistem Deteksi Intrusi melalui pelatian Jaringan Syaraf Tiruan mengunakan Algoritma Principal Component Analisys. Sedangkan sararan dari penelitian ini adalah untuk meningkatkan dan mengoptimasi kinerja Router dan Firewall dalam memonitoring dan mencegah adanya serangan maupun penyusupan ke komputer server maupun client dan membuat traffic jaringan menjadi lancar dan aman.

2. Sistem Deteksi Intrusi Dan Set Data KDD

2.1. Intrusion Detection System (IDS)

Sistem Deteksi Intrusi (IDS) masih menjadi pilihan utama bagi administrator keamanan data dan jaringan karena beberapa alasan, termasuk tidak adanya sistem yang sepenuhnya aman tanpa kekurangan atau kerentanan [11]. Jenis-jenis intrusi yang penting meliputi upaya pembobolan, penetrasi sistem kontrol keamanan, kebocoran informasi, Denial of Service (DNS), Penyamaran, penggunaan Berbahaya, dll. IDS dapat mendeteksi sebagian besar jenis serangan ini dan membantu studi dan analisis lebih lanjut, serta menambal sistem keamanan. Di antara dua jenis utama IDS, yaitu berbasis kejanggalan (Anomali) dan berbasis Penyalahgunaan (Misuse), IDS berbasis Anomali memiliki keunggulan dalam mendeteksi variasi serangan yang baru, bahkan yang kecil sekalipun, [8]. Teknik Kecerdasan Buatan seperti ANN, SVM, HMM, dll. sering digunakan untuk IDS guna mendeteksi serangan baru. Jaringan Syaraf Tiruan Multi-Layer Perceptron (MLP) digunakan sebagai algoritma IDS untuk klasifikasi berbagai jenis serangan. Sistem jaringan saraf tiruan membutuhkan set data untuk pelatihan, yang harus mencakup lalu lintas normal maupun lalu lintas serangan. Set data evaluasi IDS KDD Cup 1999 digunakan karena merupakan set data standar bagi para peneliti di bidang keamanan data dan jaringan [10].

2.2. Deskripsi Set Data KDD Cup 1999

KDDCUP’99 adalah kumpulan data yang paling banyak digunakan untuk evaluasi metode deteksi anomali. Kumpulan data ini mencakup kategori serangan berikut [14]:

2.2.1. Denial Of Service Attack (DoS Attack)

Serangan terhadap jaringan dimana Penyerang mencoba mengirim beberapa paket berbahaya, bisa berupa TCP, UDP, atau ICMP, untuk memenuhi memori atau membuat Sumber daya komputasi yang sangat sibuk untuk menangani akses pengguna yang sah ke suatu mesin.

2.2.2. User to Root (U2R)

Merupakan jenis serangan di mana peretas mencoba mendapatkan akses ke akun root sistem target, dimulai dengan akses ke akun pengguna biasa, dengan bantuan kode atau metode eksploitasi yang memanfaatkan kerentanan.

2.2.3. Remote To Local (R2L)

Dalam jenis serangan ini, penyerang yang tidak memiliki akun di mesin target, mengeksploitasi beberapa kerentanan dan mencoba mendapatkan akses ke mesin target tersebut.

2.2.4. Probing Attack

Merupakan kelas eksploitasi di mana peretas jahat mencoba mengumpulkan informasi tentang jaringan komputer.

Kumpulan data KDD CUP 99 terdiri dari 41 fitur untuk setiap paket. Tabel 1 menunjukkan deskripsi fitur dari semua fitur dalam kumpulan data KDD CUP 99. Kumpulan data tersebut diproses terlebih dahulu sebelum diterapkan pada JST agar hanya berisi nilai numerik, tetapi bukan nilai string.

Tabel 1

Fitur set data KDD Cup 1999

No.	Feature	No.	Feature
1	Duration	22	Is Guest Login
2	Type Protocol	23	Count
3	Service	24	Srv Count
4	Flag	25	Serror Rate

e-ISSN: 2798-9593
p-ISSN: 2798-9836

5	Src Bytes	26	Srv Serror Rate
6	Dsc Bytes	27	Rerror Rate
7	Land	28	Srv Rerror Rate
8	Wrong Fragment	29	Same Srv Rate
9	Urgent	30	Diff Srv Rate
10	Hot	31	Srv Diff Host Rate
11	Num Failed Logins	32	Dst Host count
12	Logged In	33	Dst Host Srv Count
13	Num Compromissed	34	Dst Host Same Srv Rate
14	Root Shell	35	Dst Host Diff Srv Rate
15	Su Attempted	36	Dst Host Same Src Port Rate
16	Num Root	37	Dst Host Srv Diff Host Rate
17	Num File Creations	38	Dst Host Serror Rate
18	Num Sell	39	Dst Host Srv Serror Rate
19	Num Access Files	40	Dst Host Rerror Rate
20	Num Outbounds Ends	41	Dst Host Srv Rerror Rate
21	Is Host Login		

2.3. Pemilihan Set Data untuk Aktivitas

Dataset KDD cup 1999 [22] terdiri dari dua berkas, yaitu 10% KDD dan terkoreksi. Untuk heterogenitas data, kami mengambil sampel pelatihan dari kedua berkas ini seperti yang ditunjukkan pada Tabel 2.

Tabel 2

Jumlah sampel yang dipilih dari set data KDD Cup 1999

Attack Main Class	**Sub Class**	**S. No of Class**	**No of Data set taken for Training From 10% KDD + From Corrected.**	**No. of data sets taken for Testing From 10% KDD + From Corrected.**
Normal	Normal	1	15,000	15,000
DOS Attacks	Smurf	2	25,000	25,000
	Neptune	3	15,000	15,000
	Back	4	1000	1000
	Mailbomb	5	4000	1000
	Teardrop	6	512	412
R2L	Snmpgetattack	7	5000	2000
	Warezmaster	8	1020	420
	Guess_passwd	9	3050	1040
	Warezclient	**10**	1000	500
U2R	Snmpguess	**11**	1500	500
Probe	Ipsweep	**12**	800	600
	Portsweep	**13**	1000	700
	Saint	**14**	600	300
	Satan	**15**	2000	1100
			76374	**65,572**

3. Jaringan Syaraf Tiruan (JST)

3.1. Jaringan Syaraf Tiruan

Keunggulan utama penggunaan JST adalah sifat nonliniernya [2], menyediakan pemetaan input-output dengan belajar bersama seorang pengajar, dapat beradaptasi dengan perubahan lingkungan, memberikan respons berbasis bukti, toleran terhadap kesalahan, dapat diimplementasikan dengan Very Large Scale Integration (VLSI), dan yang terpenting, terinspirasi oleh neurobiologis [19]. Di antara berbagai jenis jaringan saraf, multilayer perceptron (MLPNN) adalah yangpaling cocok untuk mengimplementasikan pengklasifikasi multikelas [16].

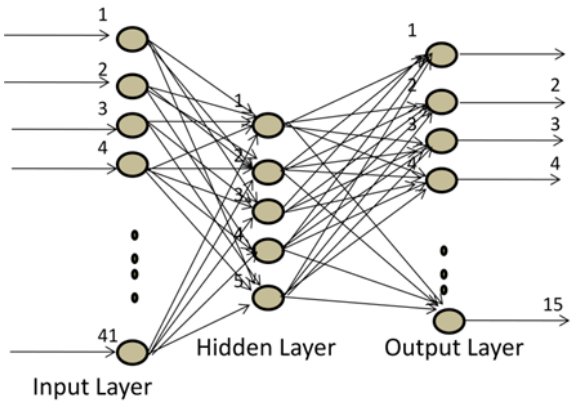
3.2. Jaringan Saraf Umpan Maju (Feed Forward):

Jaringan saraf tiruan umpan-maju multilapis memiliki beberapa neuron yang terstruktur dalam lapisan-lapisan seperti lapisan masukan, tersembunyi, dan keluaran. Lapisan keluaran dengan satu atau banyak neuron menyediakan keluaran untuk satu atau banyak masukan. Dalam satu contoh neuron, tugas proses pelatihan adalah menemukan bobot yang tepat untuk koneksi neuron yang, jika dikombinasikan dengan masukan, akan mencapai keluaran yang diinginkan. Proses ini dilakukan dengan algoritma propagasi balik.[1] Peneliti menggunakan kode Matlab untuk menjalankan algoritma JST, tetapi tidak menggunakan aplikasi alat bantu untuk hal ini.

3.2.1. Jaringan Syaraf Tiruan Multi Layer Perceptron sebelum menerapkan PCA adalah [41-5-15] yaitu:

1. Berisi 41 neuron input untuk setiap fitur input dalam dataset KDD.
2. Lima neuron tersembunyi dipilih berdasarkan metode coba-coba.
3. Lima belas neuron keluaran untuk menentukan tipe normal atau serangan.

e-ISSN: 2798-9593
p-ISSN: 2798-9836



Gbr 1. Arsitektur Jaringan Syaraf MLP.

3.2.2. Algoritma JST MLP

LANGKAH 1: MULAI

LANGKAH 2: Inisialisasi jumlah neuron tersembunyi dan epoch.

LANGKAH 3: Muat data masukan yang telah diproses sebelumnya untuk pelatihan.

LANGKAH 4: Hasilkan bobot awal neuron secara acak

LANGKAH 5:

For i=1 ke N epoch

For j=1 ke N pola masukan

- Pilih pola acak
- Hitung keluaran lapisan tersembunyi dengan menggunakan rumus berikut:

$$H_j = \frac{1}{1+e^{-\sum_{i=0}^{numInput}(W1_{i,j}.X_i)}} \quad \text{..... (1)}$$

- Sesuaikan bobot lapisan tersembunyi
- Hitung keluaran lapisan keluaran dengan menggunakan rumus berikut:

$$O_j = \frac{1}{1+e^{-\sum_{i=0}^{numHidden}(W2_{i,j}.H_i)}} \quad \text{.....(2)}$$

- Hitung kesalahan pada keluaran neuron

$$\Delta W_j = O_j(1-O_j)(T_j - O_j) \text{..... (3)}$$

For j=1 To num_Hidden,

di mana Tj adalah keluaran target yang sesuai.

- Propagasi balik kesalahan dan hitung kesalahan pada unit tersembunyi sebagai berikut:

$$\Delta V_j = H_j(1-H_j)(\Delta w.W2_j) \text{....(4)}$$

- Sesuaikan bobot keluaran neuron tersembunyi berdasarkan kesalahan
- Sesuaikan bobot masukan neuron tersembunyi akhiri loop
- if error < 0.001 end loop

LANGKAH 6: STOP

Pada akhir proses pelatihan, bobot dibekukan dan model JST akan dimulai.

4. Optimasi Fitur Menggunakan PCA

Optimasi fitur dilakukan untuk mengurangi redundansi fitur. Analisis Komponen Utama digunakan untuk tujuan ini. Dalam PCA, pemilihan fitur dilakukan untuk memilih subset fitur yang relevan, sehingga meningkatkan kinerja sistem. Dengan menghilangkan sebagian besar fitur yang tidak relevan dan redundan dari data, pemilihan fitur membantu meningkatkan kinerja model pembelajaran.

Penggunaan PCA dalam optimasi menghasilkan komponen-komponen utama, yang jumlahnya kurang dari atau sama dengan jumlah komponen sebenarnya. PCA adalah multi varian berbasis vektor Eigen. Seringkali, operasinya dapat dianggap sebagai pengungkapan struktur internal data dengan cara yang paling baik menjelaskan varians dalam data. Dengan visualisasi koordinat himpunan data multivariat dalam ruang data berdimensi tinggi (1 sumbu per variabel), PCA dapat memberikan pengguna gambaran berdimensi lebih rendah, sebuah "bayangan" dari objek ini. Hal ini dilakukan dengan hanya menggunakan beberapa komponen utama pertama sehingga dimensionalitas data yang ditransformasi berkurang. Berikut ini rumus umum untuk menghitung skor pada komponen pertama yang diekstraksi (dibuat) dalam analisis komponen utama:

C1 = b 11(X1) + b12(X 2) + ... b1p(Xp) ---(5)

Dimana:

C1 = skor subjek pada komponen utama 1 (komponen pertama yang diekstraksi)

b1p = koefisien regresi (atau bobot) untuk variabel teramati p, seperti yang digunakan dalam pembuatan komponen utama 1

Xp = skor subjek pada variabel p yang diamati

4.1. Algoritma PCA

LANGKAH 1: Dapatkan beberapa data

(Sebanyak 41 fitur dari dataset KDD CUP 99 yang terkumpul diterapkan ke PCA untuk optimasi fitur pada 41 fiturnya yang redundan dan berkorelasi).

LANGKAH 2: Kurangi rata-rata

Rata-ratanya dihitung menggunakan rumus di bawah ini:

e-ISSN: 2798-9593
p-ISSN: 2798-9836

Sekarang, rata-rata dikurangi dari setiap dimensi dalam himpunan data. Rata-rata yang dikurangi adalah rata-rata di setiap dimensi. Himpunan data yang dihasilkan dengan rata-rata yang dikurangi akan memiliki rata-rata nol.

LANGKAH 3: Hitung matriks kovariansi

Matriks kovarians akan berdimensi dua karena datanya berdimensi dua. Matriks kovarians dihitung dengan:

$$var(X) = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(X_i - \bar{X})}{(n-1)} \quad \text{----- (7)}$$

LANGKAH 4: Hitung vektor Eigen dan nilai Eigen dari matriks kovarians

Untuk menghasilkan sinyal, perlu dihitung vektor Eigen dan nilai Eigen untuk matriks ini, karena merupakan matriks persegi.

LANGKAH 5: Membentuk vektor fitur dengan memilih komponen:

Bergantung pada sinyal yang dihasilkannya, sebaiknya dipilih fitur yang nilai sinyalnya lebih besar dan fitur ini disebut komponen utama.

LANGKAH 6: Dapatkan data baru

Dengan cara mengalikan komponen yang diperoleh dengan data lama, sehingga diperoleh data baru.

5. Hasil dan Kesimpulan

5.1. Hasil

Tabel 3 menunjukkan tingkat deteksi dan tingkat positif kesalahan yang diperoleh dari pengklasifikasi JST 15 kelas untuk berbagai kelas serangan sebelum menerapkan PCA.

Tabel 3

Tingkat Deteksi MLP JST sebelum menerapkan PCA.

Attack Type	**Detection Rate**	**False Positives**
Normal	99.53	0.470
Smurf (DOS)	98.76	1.24
Neptune (DOS)	95.42	3.28
Back (DOS)	88.54	6.70
Mailbomb (DOS)	86.91	9.62
Teardrop (DOS)	77.32	15.61
Snmpgetattack(R2L)	90.10	7.9
warezmaster(R2L)	78.24	13.21
Guess_passwd(R2L)	87.21	8.43
Warezclient(R2L)	80.41	13.11
snmpguess(U2R)	81.17	12.10
ipsweep(Probe)	82.87	10.25
portsweep(Probe)	84.32	11.21
saint(Probe)	73.23	17.55
satan(Probe)	90.34	5.56
Average	**86.28%**	

Tabel 4 menunjukkan keluaran PCA yang berhasil memilih 15 fitur teratas yang lebih efektif.

Tabel 4

15 fitur teratas yang dipilih dari PCA.

Feature Rank	Feature number out of 41 features	Feature name	Output of PCA Signal value
1	5	Src bytes	9.913595
2	33	Dst host srv count	8.638142
3	32	Dst host count	5.380869
4	3	Service	5.380742
5	2	Protocol type	5.379961
6	4	Flag	5.377820
7	29	Same srv rate	5.369393
8	34	Dst host same srv rate	5.356421
9	36	Dst host same src port name	5.354023
10	12	Logged in	5.306561
11	38	Dst host serror rate	5.288926
12	37	Dst host serv diff host name	5.288926
13	35	Dst host diff serv rate	5.258945
14	1	Duration	5.117015
15	31	Srv diff host rate	3.201556

Tabel 5 dan 6 menunjukkan matriks confusion yang sesuai. Hasilnya jelas menunjukkan bahwa tingkat deteksi bergantung pada jumlah set pelatihan yang tersedia karena dari Tabel 1 kita dapat melihat bahwa rekaman untuk beberapa jenis serangan seperti Tear drop, warezmaster, saint, dll. lebih sedikit jumlahnya, demikian pula tingkat deteksinya.

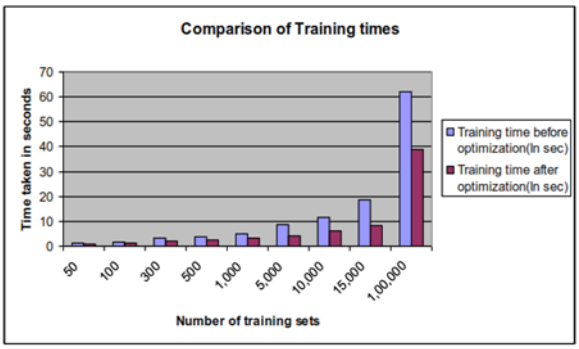
e-ISSN: 2798-9593
p-ISSN: 2798-9836

Tabel 5.

Waktu pelatihan MLP JST untuk berbagai jumlah set data.

Number of Training Sets	Training time before optimization(In sec)	Training time after optimization(In sec)
50	1.2216	0.9824
100	1.7521	1.3400
300	3.2733	1.9654
500	3.8845	2.4121
1,000	5.1320	3.1120
5,000	8.6560	4.2631
10,000	11.5410	6.1825
15,000	18.6718	8.2123
1,00,000	62.1300	38.9290

Gbr. 2. menunjukkan perbandingan waktu pelatihan JST sebelum dan sesudah menerapkan PCA untuk mereduksi fitur.



Gbr 2. Grafik Waktu Pelatihan untuk perbandingan sebelum dan sesudah PCA.

Tingkat deteksi yang lebih rendah pada beberapa kelas disebabkan oleh fakta bahwa kumpulan data untuk pelatihan sangat terbatas.

Tabel 6

Tingkat Deteksi MLP JST setelah menerapkan PCA.

Attack Type	Detection Rate	False Positives
Normal	99.61	0.39
Smurf (DOS)	98.58	1.42
Neptune (DOS)	95.81	2.83
snmpguess(U2R)	81.22	12.3
ipsweep(Probe)	84.10	9.81
Warezclient(R2L)	80.29	12.76
Snmpgetattack(R2L)	90.72	6.77
warezmaster(R2L)	80.17	11.68
Guess_passwd(R2L)	87.60	8.11
portsweep(Probe)	85.21	10.84
saint(Probe)	74.54	16.65
satan(Probe)	91.14	5.20
Total	**88.31%**	
Back (DOS)	90.16	6.12
Mailbomb (DOS)	88.13	8.64
Teardrop (DOS)	78.14	13.18

5.2. Kesimpulan

Hasil pelatihan dan pengujian menunjukkan bahwa Analisis Komponen Utama terbukti merupakan teknik yang sangat efisien yang dapat digunakan untuk reduksi dimensionalitas data tanpa kehilangan orisinalitas set data. Jaringan saraf tiruan MLP telah terbukti dapat mengimplementasikan masalah klasifikasi multikelas dengan sangat efisien bahkan dengan 15 kelas. Dalam penelitian ini, telah didemonstrasikan kapabilitas JST dalam klasifikasi outlier terperinci terkait dengan set data Sistem Deteksi Intrusi. Tabel 5 menunjukkan peningkatan 62% dalam efisiensi pelatihan terkait waktu yang dihabiskan, yang merupakan peningkatan yang sangat signifikan.

Ucapan Terima Kasih

Terimakasih penulis ucapkan kepada pihak-pihak yang terkait dengan penelitian yang telah dilaksanakan terutama kepada pihak pejabat yang ada di LPPM Universitas Mandiri Bina Prestasi yang telah mengeluarkan surat pelaksanaan penelitian sehingga semua prosedur dan pelaksanaan penelitian dapat berjalan dengan lancar. Kami penulis juga mengucapkan terimakasih kepada Universitas Mandiri Bina Prestasi serta teman-teman peneliti yang telah mendukung pelaksanaan penelitian hingga publikasi ke jurnal terakreditasi.

Referensi

[1] Ravi Kiran Varma.P, V.Valli Kumari, VVS. Prasanna, “Heuristic approach to improve the performance of ANN based Intrusion Detection System ”, Proceedings of the 3rd.
[2] Srinivas Mukkamala, Intrusion detection using neuralnetworks and support vector machine, Proceedings of the2002 IEEE International Honolulu, HI, 2002.
[3] J.P Anderson. Computer Security Threat Monitoring andSurveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.
[4] Fariba Haddadi, Sara khanchi, Mehran Shetabi, Vali Derhami “Intrusion detection and attack classification using Feed-Forward Neural Network”, Proceedings of the Second IEEE..
[5] T.Petreus, CE Cotrutz, M. Neamtu, E.C. Buruiana, P.D. Sirbu, A. Neamtu, “Understanding the dynamics-activity relationship in metalloproteases : Idea for new inhibition strategies”, 2010 IEEE
[6] M. Moradi, Mohammad Zulkernine. A Neural Network Based System for Intrusion Detection and Classification of Attacks. Proceedings of 2010”,..
[7] Leila Mechtri, Fatiha Djemili Tolba, Nacira Ghoualmi, “Intrusion Detection Using Principal Component Analysis”, IEEE 2 nd Aug 2010.
[8] John McHugh, Alan Christie, Julia Allen, “DefendingYourself: The role of Intrusion Detection Systems”, IEEE

e-ISSN: 2798-9593
p-ISSN: 2798-9836

[9] Software, vol 17 no. 5 pp 42-51, Sep 2000. Varun Chandola, Arindam Banerjee, Vipin Kumar, "Anomaly Detection: A Survey", ACM Computing Surveys, Vol. 41, No. 3, Article 15, July 2009..
[10] Amit kumar Choudary, Akhilesh Swarup, "Neural Network Approach for Intrusion Detection", proceedings of the 2009
[11] Yana Demidova, Maksym Ternovoy, "Neural Network Approach of Attack's Detection In the Network Traffic",The IXth
[12] D. E. Denning, "An intrusion detection model," IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222–232, 1987.
[13] J. Ryan, M. Lin and R. Miikkulainen, Intrusion Detection with Neural Networks, AI Approaches to Fraud Detection and Risk Management: Papers from the 2017 AAAI
[14] K. Fox, R. Henning, J. Reed and R. Simonian, A Neural network approach towards intrusion detection, Proceedingsof ACM 13th
[15] James Cannady, Artificial neural networks for misusedetection, Proceedings of the 2011.