Jurnal CoreIT, Vol.5, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Penerapan Metode Radial Basis Function Dengan Jumlah Center Dinamis Untuk Klasifikasi Serangan Jaringan Komputer

Iwan Iskandar, Eza Resdifa
Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau
Jl. HR. Soebrantas No.155 Simpang Baru, Panam, Pekanbaru, 28293
iwan.iskandar@uin-suska.ac.id, eza.resdifa@students.uin-suska.ac.id

Abstrak **- Ancaman serangan pada jaringan merupakan masalah yang sangat banyak dan semakin pesat perkembangannya saat ini. Jaringan komputer yang kita gunakan rawan akan serangan sehingga merugikan pengguna jaringan. Beberapa contoh jenis serangan yaitu *U2R, R2L, Probes,* dan *DOS*. Untuk mengetahui jenis serangan dapat dilakukan klasifikasi terhadap serangan jaringan komputer menggunakan salah satu metode jaringan saraf tiruan. Pada penelitian ini dilakukan klasifikasi serangan jaringan komputer menggunakan metode *Radial Basis Function* (RBF) dengan jumlah *center* dinamis. Jumlah nilai *center* yang digunakan dilihat dari jumlah nilai *error* terkecil pada proses pelatihan jaringan RBF. Nilai *error* terkecil diperoleh dari hasil pelatihan dengan jumlah *center* sebanyak inputan sampai dua kali jumlah inputan. Penentuan nilai *center RBF* menggunakan algoritma *clustering* yaitu algoritma *K-means*. Data yang digunakan pada penelitian ini adalah data KDD Dataset CUP 1999. Variabel yang digunakan sebanyak 33 variabel dari 41 variabel data KDD Dataset Cup 1999. Jumlah data yang digunakan sebanyak 7047 data dengan pembagian data latih dan data uji adalah 70%:30%, 80%:20% dan 90%:10%. Parameter RBF yang digunakan adalah nilai *spread* 1 sampai 9. Hasil penelitian ini diperoleh akurasi sebesar 97,9% dengan jumlah center 59 dan nilai *spread* 1.**

Kata Kunci : Center Dinamis, Jaringan Syaraf Tiruan, KDD Dataset CUP 1999, Radial Basis Function, Serangan jaringan.

PENDAHULUAN

Jaringan komputer merupakan teknologi yang perkembangan sangat pesat saat ini. Hampir disetiap perusahaan, istansi pemerintahan, sekolah, rumah sakit, perguruan tinggi, masjid dan disetiap tempat pada saat ini umumnya terdapat jaringan komputer. Internet pada saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraksi. Tetapi dengan banyak komputer yang terhubung bisa menjadi ancaman berbahaya yang dapat menimbulkan terjadi serangan, baik dari dalam maupun luar seperti virus, trojan maupun *hacker*.

Ancaman serangan pada jaringan merupakan masalah yang sangat banyak dan semakin pesat perkembangannya saat ini. Seperti kasus yang diberitakan dari Tempo (2017) serangan jaringan komputer yang telah merugikan Bank Sentral Negara Bangladesh pada Februari 2016. Bank tersebut diretas oleh *hacker* yang dinilai memiliki hubungan dengan Korea Utara, mendapatkan $81 juta (sekitar Rp 1,08 triliun). Kompromi terhadap akun-akun Swift, digunakan untuk memindahkan uang antarnegara adalah alasan utama mengapa komputer-komputer dalam bank sentral Bangladesh bisa diretas.

Serangan-serangan pada jaringan komputer semakin berkembang dan jaringan komputer rentan dibobol sehingga merugikan pengguna jaringan. Salah satu contoh bentuk serangan seperti *Buffer Overflow, DOS attack, SMB Probes, OS Fingerprint* dan lain-lain [1]. Serangan dapat membuat tiga aspek penting dalam jaringan komputer menjadi terganggu yaitu: penyusup mempunyai akses ke informasi atau data rahasia, keaslian informasi dapat dimodifikasi oleh penyerang dan ketersedian akan informasi menjadi tidak dapat digunakan secara normal [2].

KDD *(Knowledge Discovery and Data Mining) dataset Cup* 1999 merupakan salah satu contoh data serangan jaringan yang berhasil ditangkap pada jaringan komputer. *KDD dataset Cup* merupakan *dataset* yang dikeluarkan oleh DARPA (*Defense Anvance Research Project Agency*) pada tahun 1998. Data ini digunakan sebagai versi data kompetisi di bidang Data Mining dan Ekplorasi ilmu pengetahuan diseluruh dunia yang diadakan oleh *ACM SIGKDD* (*Special Interest Group on Knowledge Discovery and Data Mining*). Fitur yang ada pada KDD *dataset* Cup 99 terdiri dari 41 fitur terdiri dari fitur kategoris dan numerik[7]. Pada data KDD dataset cup 1999 terdapat jenis serangan Probes, DOS, U2R, R2L dan bukan serangan [8].

Untuk mengetahui jenis serangan jaringan seperti Probes, DOS, U2R, R2L dan bukan serangan dapat dilakukan klasifikasi menggunakan mesin learning. Pada beberapa penelitian klasifikasi serangan jaringan computer menggunakan mesin learning dilakukan dengan pembelajaran Data Mining dan Jaringan Syaraf Tiruan.

Pada penelitian ini dilakukan klasifikasi serangan jaringan komputer dengan pembelajaran

Jarinngan Syaraf Tiruan (JST). JST merupakan suatu model kecerdasan yang diilhami dari struktur otak manusia dan kemudian diimplementasikan menggunakan program komputer yang mampu menyelesaikan sejumlah proses perhitungan selama proses pembelajaran berlangsung [3]. Beberapa metode yang biasa diterapkan dalam jaringan syaraf tiruan untuk klasifikasi serangan jaringan komputer adalah *Learning Vector Quantization* (LVQ), *Error Backpropagation* (EBP), *Self Organizing Map* (SOM), *Feed Forward Neural Network* (FFNN), *Elman Neural Network* (ENN), *Generalized Regression Neural Network* (GRNN), *Probabilistic Neural Network* (PNN), *Feed Forward Neural Network* (FFNN) dan *Radial Basis Function* (RBF).

Pada penelitian ini digunakan metode RBF untuk melakukan klasifikasi pada serangan jaringan komputer. Metode *Radial Basis Function* merupakan struktur jaringan sederhana yang tidak perlu menggunakan perhitungan panjang. RBF Neural Network memiliki kemampuan untuk mempelajari sesuatu dengan cepat. Dalam pendekatan klasik metode *RBF Neural Network* memiliki *hidden layer* didapat dari *input* data. Struktur jaringan *RBF Neural Network* terdiri dari tiga lapisan yaitu *input layer, hidden layer* dan *output layer* [9].

Beberapa penelitian terkait menggunakan metode RBF pada klasifikasi serangan jaringan komputer dilakukan oleh Kashyap Suresh dkk, pada tahun 2013 pada penelitian tersebut dilakukan pebandingan antara metode RBF dengan metode EBP, menghasilkan kesimpulan bahwa metode RBF lebih baik dibandingkan dengan metode EBP. Kemudian penelitian oleh Devaraju S dan Ramakrishnan S, pada tahun 2013 menyatakan bahwa RBF mencapai tingkat akurasi sebesar 83,51%.

Pembentukan struktur jaringan pada RBF ditentukan oleh 3 buah parameter yang dapat disesuaikan yaitu titik pusat dan lebar jarak antara *hidden layer* dan bobot koneksi dari *hidden layer* ke *output layer*. Jumlah nilai *center* yang digunakan pada jaringan RBF yaitu sejumlah inputan sampai dua kali jumlah inputan [12]. Jumlah nilai center yang diguanakan pada jaringan RBF adalah dilihat dari jumlah nilai eror terkecil pada proses pelatihan jaringan RBF. Penentuan nilai *center RBF* dilakukan dengan dua acara, secara acak dan menggunakan algoritma clustering.

Algortima *clustering* yang digunakan dalam menentukan nilai *center* yaitu menggunakan algoritma K-Means dan C-means. Pada penelitian ini penulis mengggunakan algoritma K-means dalam menentukan nilai center. Algoritma K-Means adalah proses pencarian center terbaik untuk jaringan syaraf tiruan yang terbentuk dan clustering data sesuai nilai center [10]. Kemudian, algoritma K-means merupakan algoritma yang sering digunakan dalam pencarian nilai center [11].

Berdasarkan beberapa penelitian sebelumnya pada penelitian ini akan dilakukan penerapan algoritma RBF dengan jumlah center dinamis pada klasifikasi serangan jaringan komputer. Data serangan komputer yang digunakan bersumber dari KDD *dataset Cup* 1999. Diharapkan dalam penelitian ini, dapat mengklasifikasikan jenis serangan komputer lebih baik dan memiliki nilai akurasi tinggi.

1. *Radial Basis Function*

Jaringan fungsi *Radial Basis Function* (RBF) yang merupakan alternatif dari jaringan *Multilayered Feedforward Neural* (MFN) yang telah dikembangkan. Jaringan ini terdiri dari 3 layer yaitu *input layer, hidden layer*, dan *output layer*, dimana hanya memiliki satu unit pada *hidden layer*. Jumlah *hidden layer* dari jaringan RBF adalah sejumlah inputa sampai 2 kali inputan. Fungsi aktivasi adalah fungsi basis dan fungsi linear pada lapisan *output*. Jaringan ini telah banyak digunakan secara intensif. RBF merupakan fungsi tak linier *multidimesional* yang tergantung pada jarak vektor *input* dan vektor *center*. RBF dengan input berdimensi-m dan output berdimensi-n.

Algoritma JST RBF adalah:

a. Menentukan pusat data dari data latih.
   Dalam menentukan pusat data dilakukan dengan pengambilan nilai center secara acak diambil dari nilai inputan pada proses pelatihan dan menggunakan algoritma *clustering*.
b. Menghitung jarak *Eucledian*
   $\| x_i - x_k \| = D_{i,k} = \sqrt{\sum_{j=1}^{p}(x_{i,j} - x_{k,j})^2}$ (1)
   Dimana i,k = 1,2…….n, j= 1, 2, ….p
c. Menghitung fungsi gaussian hasil aktivasi dengan fungsi basis radial dari jarak data dikalikan b1;
   $\varphi_{i,k} = e^{-(b1*D_{i,k})^2}$ (2)
   Dengan : b1 = $\frac{\sqrt{-\ln(0,5)}}{\sigma(spread)}$, *spread* merupakan bilangan *real* positif
d. Menghitung bobot pelatihan dengan menggunakan persamaan
   $w = (G^T G)^{-1} G^T d$ (3)
e. Menghitung *output* JST RBF dengan menggunakan persamaan
   $y = \sum \varphi\, w + b$ (4)
f. Menghitung galat (*error*) antara *output* hasil pelatihan dengan target. Persamaannya yaitu:
   $error = t_k - y_k$ (5)
   Keterangan rumus:
   x_i = vektor *input* data
   x_k = vektor *center*
   φ = fungsi *Gaussian*
   σ = nilai *spread*
   w = nilai bobot
   b = bias
   G = inisialisasi nilai Gaussian (φ)
   d = vektor target

y = *output* rbf

2. Algoritma *K-Means*

K-Means adalah algoritma *clustering* untuk data mining yang diciptakan tahun 70-an dan berguna untuk melakukan clustering secara *unsupervised learning* (pembelajaran tidak terawasi) dalam kumpulan data berdasarkan parameter-parameter tertentu. *K-Means* mengelompokkan objek menjad K kluster.

Berikut adalah langkah-langkah dalam memproses algoritma *K-means*:

a. Tentukan jumlah k-*cluster* yang diinginkan
b. Lakukan inisialisasi untuk menentukan pusat *cluster*
c. Hitung *centroid* rata-rata dari data berdasarkan data keluarga yang bergabung pada setiap cluster dengan persamaan

$$C_{ik} = \frac{1}{M}\sum_{j}^{M} X_j \quad (6)$$

d. Untuk tiap baris, tentukan pusat *cluster* yang terdekat. Untuk menghitung *distance* atau jarak antara data dengan pusat cluster digunakan rumus *Distance Euclidian*

$$D(X_i, C_j) = \left|\left|X_i - C_j\right|\right| = \sqrt{\sum_{j=1}^{n} |x_{1j} - C_{1j}|^2} \quad (7)$$

e. Menentukan grup berdasarkan jarak terpendek.
f. Untuk tiap *k-cluster*, temukan *centroid* (*means*) dari *cluster* tersebut dan *update* lokasi dari pusat *cluster* kedalam nilai *centroid* baru

$$Mk = \frac{1}{N_k} X \sum_{j=1}^{N_k} X_{jk} \quad (8)$$

g. Ulangi langkah ketiga sampai e hingga batas nilai iterasi atau nilai tolerasnsi yang ditentukan masih ada data yang berpindah.

3. Normalisasi

Normalisasi dilakukan untuk merubah nilai-nilai fitur dari dataset KDD Cup 1999. Data dalam penggunaan *Artificial Neural Network* harus dilakukan proses normalisasi dengan skala tertentu agar ANN dapat bekerja maksimal (Sarda P, Dr. Sadgir P, 2015). Ini bertujuan untuk perhitungan *Euclidean*, karena atribut yang ber-skala panjang dapat mempunyai pengaruh yang lebih besar dari pada atribut dengan skala pendek. Oleh karena itulah dibutuhkan Normalisasi untuk mencegahnya. Rumus normalisasi yang digunakan adalah:

$$x = \frac{0{,}8\ x\ (x_p - \min(x_p))}{\max(x_p) - \min(x_p)} + 0{,}1 \quad (9)$$

Dimana:

x` : hasil nilai normalisasi
x_i : data ke i (1,2,3,4.....,i)
min(x) : nilai minimum pada atribut x
max(x) : nilai maksimum pada atribut x

4. KDD *Dataset CUP* 1999

KDD dataset Cup merupakan *dataset* yang dikeluarkan oleh DARPA (*Defense Anvance Research Project Agency*) pada tahun 1998. DARPA dataset merupakan contoh lalu lintas jaringan dan log audit sebuah simulasi jaringan militer yang digunakan untuk mengevaluasi deteksi intrusi sistem. Data ini dikumpulkan pada tahun 1998 oleh Informasi Kelompok Teknologi Sistem Laboratorium MIT Lincoln. Kdd dataset cup 1999 memilki 41 fitur terdiri dari fitur kategories dan numerik.

5. *Confusion Matrix*

Confusion matrix adalah alat yang berguna untuk menganalisis seberapa baik classifer mengenali tuple dari kelas yang berbeda. *Confusion Matrix* pada penelitian digunakan untuk menghitung tingkat akurasi. Menghitung tingkat akurasi merupakan hal terpenting dalam sebuah penelitan agar dapat diketahui tingkat keberhasilan dan kegagalan dalam sebuah penelitian. Pada confusion matrix terdapat istilah TP dan TM yang memberikan informasi ketika classifer benar dan FP dan FN memberikan informasi ketika classifer salah [4].

Contoh *confusion matrix* untuk klasifikasi biner ditunjukkan pada tabel 1 berikut.

Tabel 1. Confusion Matrix

		Kelas Prediksi	
		1	0
Kelas Sebenarnya	1	TP	FN
	0	FP	TN

Akurasi merupakan persentase dari data yang diprediksi secara benar. Perhitungan akurasi adalah:

$$\text{Akurasi} = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (10)$$

Error = 100% - Akurasi (11)

Keterangan:

TP : *True Positives*, merupakan jumlah data dengan kelas positif yang diklasifikasikan positif.
TN : *True Negative*s, merupakan jumlah data dengan kelas negatif yang diklasifikasikan negatif.
FP : *False Positives*, merupakan jumlah data dengan kelas positif yang diklasifikasikan negatif.
TP : *True Positives*, merupakan jumlah data dengan kelas negatif yang diklasifikasikan positif.

TAHAPAN ANALISA

Aplikasi penerapan metode *Radial Basis Function* untuk meng-klasifikasi serangan pada jaringan memiliki 3 proses dalam meng-klasifikasi serangan, yaitu: analisa data, analisa algortima RBF dengan jumlah center dinamis dan analisa aplikasi

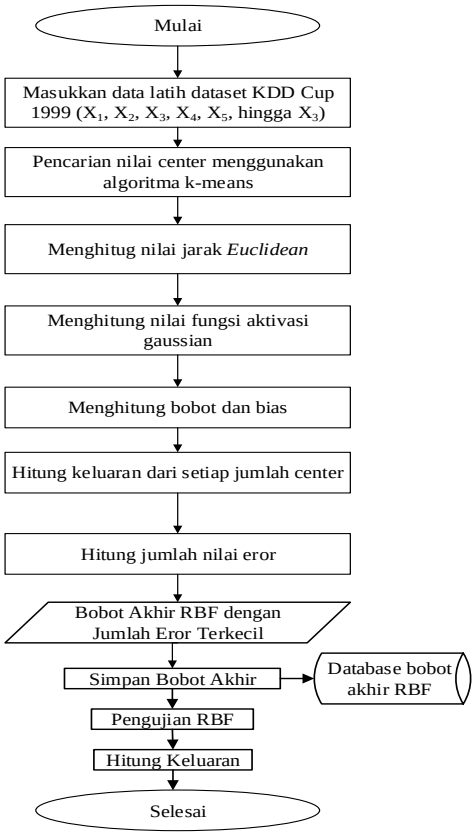
1. Analisa Data

Tahapan analisa data adalah melakukan analisa terhadap data yang telah dikumpulkan. Analisa data terbagi atas empat yaitu:

a. *Selection Data*
   Pada tahapan *selection* data ini dilakukan pemilihan variabel yang akan digunakan pada klasifikasi serangan jaringan komputer.
b. *Preprocessing* data
   Pada tahapan *preprocessing* akan dilakukan ekstraksi data terhadap data yang akan digunakan untuk data pelatihan, sehingga membentuk fitur-fitur yang dapat digunakan dengan baik dalam proses pelatihan menggunakan RBF. Pada tahapan ini dilakukan menghapus *missing value*, menghapus duplikat data, transformasi data, normalisasi data menggunakan rumus 2.11 dan penghapusan data *outlayer*.
c. Data latih
   Data latih adalah data yang digunakan sebagai standarisasi dalam melakukan pengujian aplikasi
d. Data uji
   Data uji merupakan data yang digunakan untuk pengecekan hasil dari data latih.

2. Analisa Algoritma RBF dengan Jumlah *Center* Dinamis

Pada tahapan analisa algoritma RBF menggunakan *center* dinamis. Pada gambar 1 berikut adalah tahapan analisa metode RBF:



Gambar 1 Tahapan Analisa Metode RBF

Keterangan gambar 1 adalah:

a. Menentukan fungsi basis. Fungsi basis ini akan digunakan untuk aktivasi fungsi di *hidden layer*. Fungsi basis yang digunakan yaitu fungsi *gaussian* yang akan menentukan bayaknya *center*. *Center* mempengaruhi arsitektur jaringan RBF karna *center* akan menjadi *neuron* pada *hidden layer* RBF.
b. Menghitung pusat nilai *center* dengan algoritma *K-Means* sejumlah inputan (n) sampai dua kali jumlah inputan (2n).
c. Menyusun arsitektur jaringan RBF
d. Pelatihan jaringan RBF
e. Inisialisasi bobot pada *hidden layer*
f. Hitung keluaran RBF
g. Hitung jumlah nilai eror dari setiap jumlah center, pilih jumlah nilai center yang memiliki eror terkecil untuk dilakukan proses pengujian.
h. Pengujian RBF
i. Hitung Keluaran
j. Hitung Akurasi

3. Analisa Aplikasi

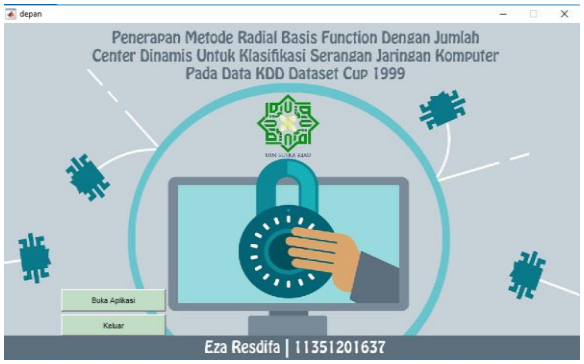
Pada tahapan analisa aplikasi menjelaskan bagaimana bentuk aplikasi yang akan dibangun, data yang digunakan, variable yang digunakan, keluaran dari aplikasi dan menu yang terdapat pada aplikasi serta menjelaskan cara kerja metode yang digunakan dalam klasifikasi serangan jaringan pada KDD Dataset CUP 1999.

Jurnal CoreIT, Vol.5, No.2, Desember 2019
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

HASIL DAN PEMBAHASAN

Langkah pertama yang dilakukan adalah meng-akses aplikasi yang telah dibuat, adapun halaman utama dari aplikasi adalah

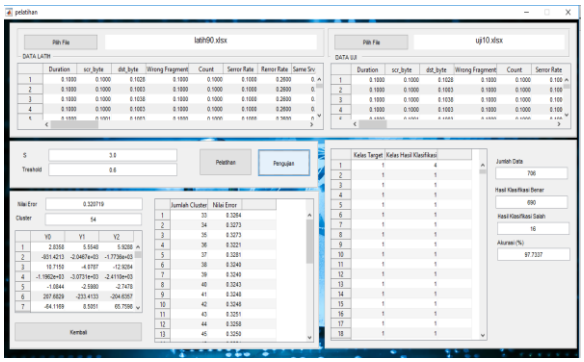
1. Halaman Utama
   Adapun halaman utama dapat dilihat pada Gambar 2:



Gambar 2 Halaman Utama

2. Halaman Pelatihan dan Pengujian

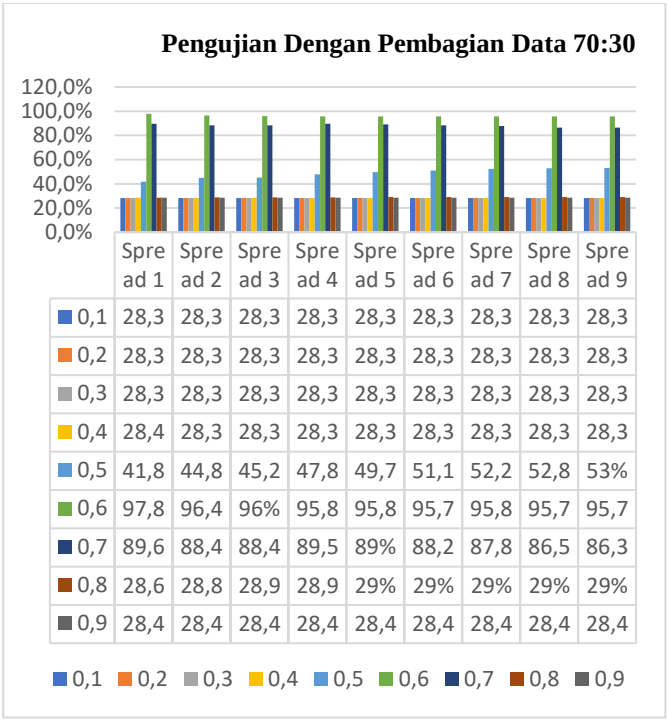
Adapun halaman data latih dapat dilihat pada Gambar 3



Gambar 3 Data Latih dan Data Uji

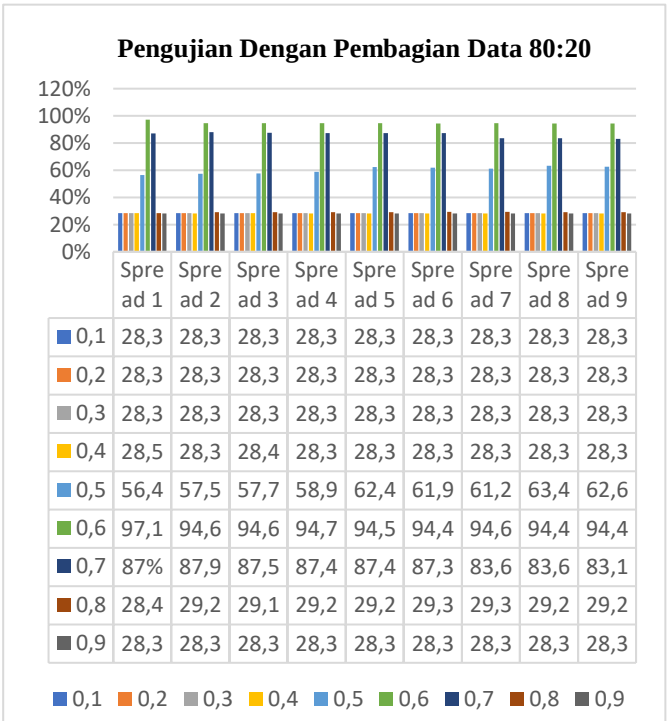
Proses pengujian dilakukan berdasarkan nilai spread, nilai treashold dan banyak data

1. Berdasarkan Nilai Spread
   Berikut grafik hasil pengujian klasifikasi serangan jaringan komputer menggunakan metode *Radial Basis Function* dengan jumlah center dinamis.



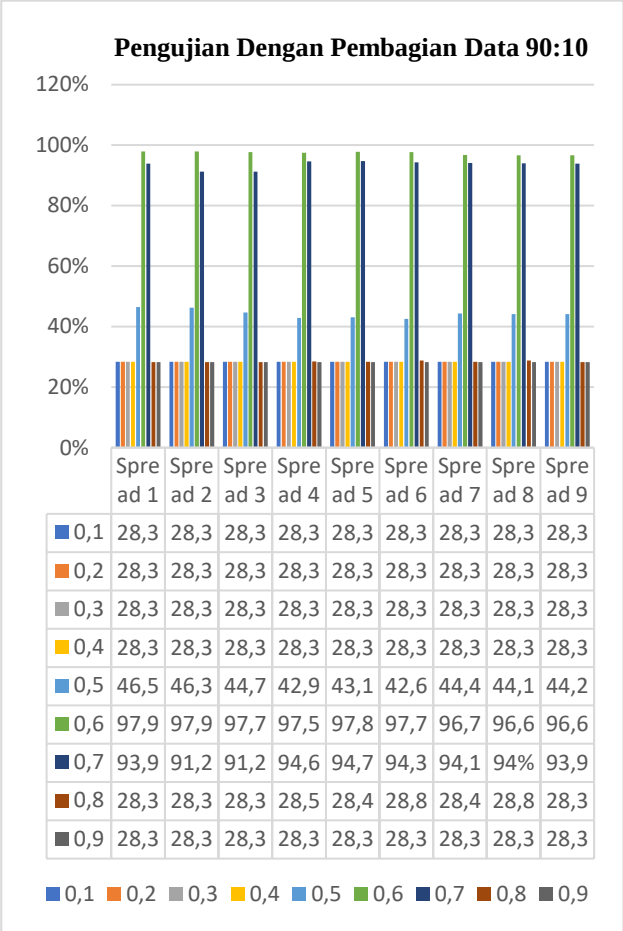
Gambar 4 Grafik Pengujian 70:30

Pada gambar 4 dapat dilihat bahwa nilai *spread* tidak mempangaruhi tingkat akurasi data. Akurasi data akan tinggi ketika nilai threshold yang diubah.



Gambar 5 Grafik Pengujian 80:20

Pada gambar 5 dapat dilihat bahwa nilai *spread* tidak mempangaruhi tingkat akurasi data. Akurasi data akan tinggi ketika nilai threshold yang diubah.

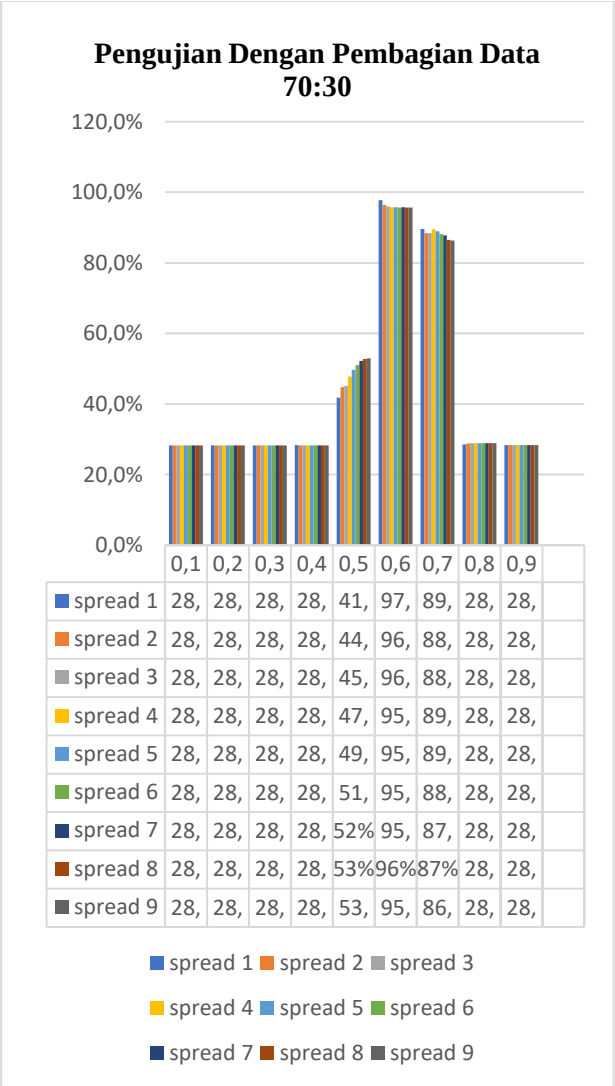


	Spread 1	Spread 2	Spread 3	Spread 4	Spread 5	Spread 6	Spread 7	Spread 8	Spread 9
0,1	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3
0,2	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3
0,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3
0,4	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3
0,5	46,5	46,3	44,7	42,9	43,1	42,6	44,4	44,1	44,2
0,6	97,9	97,9	97,7	97,5	97,8	97,7	96,7	96,6	96,6
0,7	93,9	91,2	91,2	94,6	94,7	94,3	94,1	94%	93,9
0,8	28,3	28,3	28,3	28,5	28,4	28,8	28,4	28,8	28,3
0,9	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3	28,3

Gambar 6 Grafik Pengujian 90:10

Pada gambar 6 dapat dilihat bahwa nilai *spread* tidak mempangaruhi tingkat akurasi data. Akurasi data akan tinggi ketika nilai threshold diubah.

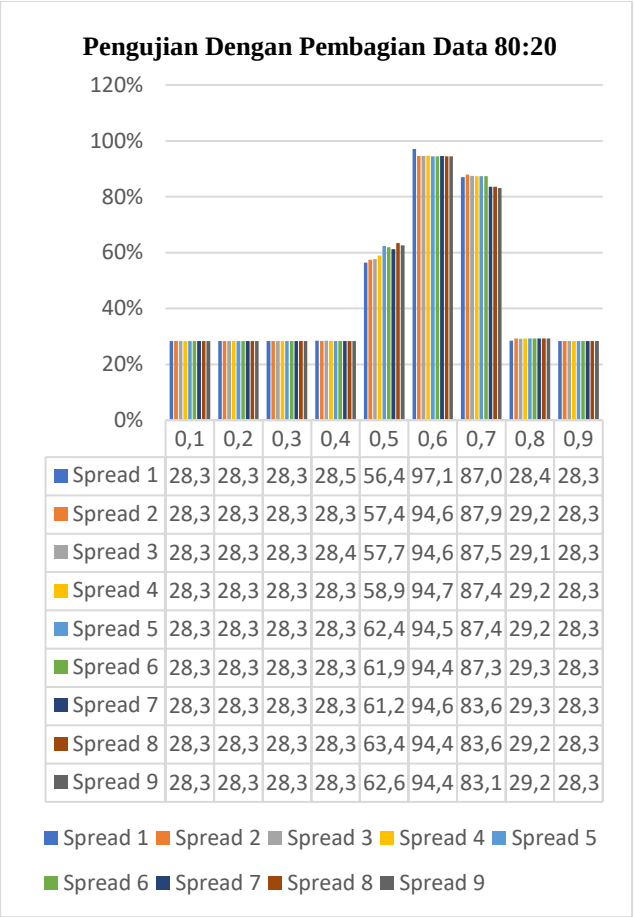
2. Berdasarkan nilai *treashold*
   Berikut ini merupakan grafik hasil dari pengujian dengan pembagian data 70:30, 80:20, dan 90:10 dengan ambang batas (*treshold*) yaitu 0,1, 0,2, 0,3, 0,4, 0,5, 0,6, 0,7, 0,8, dan 0,9 nilai *spread* 1, 2, 3, 4, 5, 6, 7, 8, dan 9. Berikut grafik hasil pengujian klasifikasi serangan jaringan komputer menggunakan metode *Radial Basis Function* dengan jumlah center dinamis.



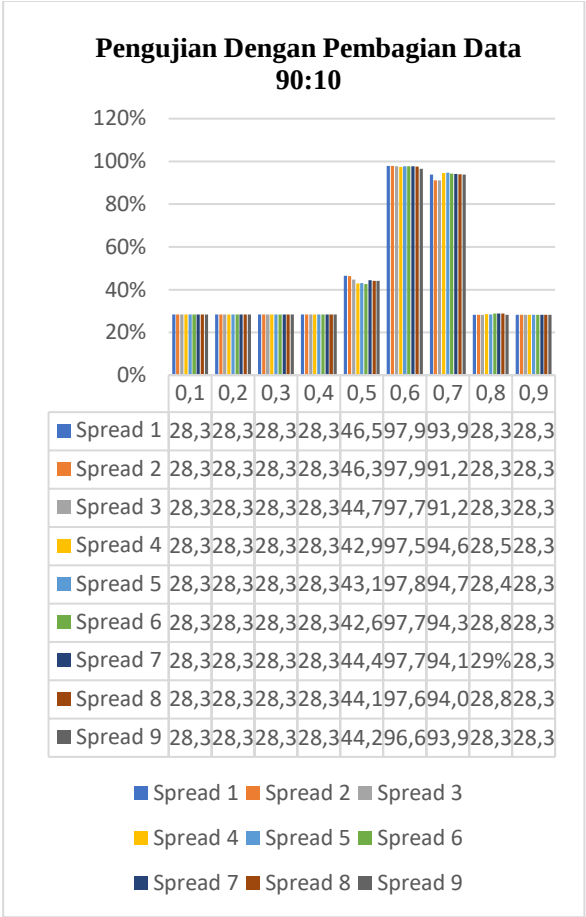
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
spread 1	28,	28,	28,	28,	41,	97,	89,	28,	28,
spread 2	28,	28,	28,	28,	44,	96,	88,	28,	28,
spread 3	28,	28,	28,	28,	45,	96,	88,	28,	28,
spread 4	28,	28,	28,	28,	47,	95,	89,	28,	28,
spread 5	28,	28,	28,	28,	49,	95,	89,	28,	28,
spread 6	28,	28,	28,	28,	51,	95,	88,	28,	28,
spread 7	28,	28,	28,	28,	52%	95,	87,	28,	28,
spread 8	28,	28,	28,	28,	53%	96%	87%	28,	28,
spread 9	28,	28,	28,	28,	53,	95,	86,	28,	28,

Gambar 7 Grafik Pengujian 70:30 Treshold

Pada gambar 7 hasil pengujian tertinggi diperoleh dengan nilai *threshold* 0,6 dengan tingkat akurasi tertinggi 97,8% pada nilai *spread* 1. Hasil pengujian terendah pada *threshold* 0,1, 0,2, 0,3, 0,8, dan 0,9 dengan tingkat akurasi 28,3% pada nilai *spread* 1 sampai 9. Pada grafik dapat dilihat akurasi akan membaik ketika nilai treshold yang digunakan adalah 0,6.



Gambar 8 Grafik Pengujian 80:20 Treshold



Gambar 9 Grafik Pengujian 90:10

Pada gambar 8 hasil pengujian tertinggi diperoleh dengan nilai *threshold* 0,6 dengan tingkat akurasi tertinggi 97,1% pada nilai *spread* 1. Hasil pengujian terendah pada *threshold* 0,1, 0,2, 0,3, 0,8, dan 0,9 dengan tingkat akurasi 28,3% pada nilai *spread* 1 sampai 9. Pada grafik dapat dilihat akurasi akan membaik ketika nilai tresholh yang digunakan adalah 0,6.

Pada gambar 9 hasil pengujian tertinggi diperoleh dengan nilai *threshold* 0,6 dengan tingkat akurasi tertinggi 97,90% pada nilai *spread* 1. Hasil pengujian terendah pada *threshold* 0,1, 0,2, 0,3, 0,8, dan 0,9 dengan tingkat akurasi 28,3% pada nilai *spread* 1 sampai 9. Pada grafik dapat dilihat akurasi akan membaik ketika nilai treshold yang digunakan adalah 0,6.

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka didapatkan kesimpulan sebagai berikut:

1. Akurasi pengujian tertinggi yaitu mencapai 97,9% pada pembagian data latih dan data uji 90:10 dengan jumlah center 59 nilai *spread* 1 dan *treshold* 0,6
2. Nilai *eror* terkecil yang didapat dari pengujian adalah 0,29% yang menghasilkan nilai akurasi diatas 80%
3. Pengaruh parameter yang diuji yaitu:
   a. Semakin banyak data latih maka akurasi semakin tinggi
   b. Nilai *Spread* tidak terlalu mempengaruhi tingkat akurasi data

c. Nilai *treshold* terbaik adalah 0,6, dengan nilai *threshold* 0,6 tingkat akurasi diatas 90%

4. Algoritma *Radial Basis Function* (RBF) dengan jumlah *center* dinamis dapat diterapkan pada klasifikasi serangan jaringan komputer pada data KDD Dataset CUP 1999.

REFERENSI

[1] Takyudin, 2012. Aplikasi Host-Based Intrusion Detection System (H-IDS) Dengan Menggunakan Metode *Adaptive Nuero Fuzzy Inference System*

[2] Soleiman. E. M dan Fetanat .A., 2014. Using Learning Vector Quantization (LVQ) in Intrusion Detection Systems. , 1(10): 15–19.

[3] Desiani Anita, Arhami Muhammad. 2005. "*Konsep Kecerdasan Buatan*", Andi: Palembang

[4] Elvianti. 2014. "*Penerapan Metode Modified K-Nears Neighboour (MKNN) Untuk Klasifikasi Penderita Penyakit Liver*", Universitas Islam Negeri Sultan Syarif Kasim Riau

[5] KDD CUP 1998 DARPA (Defense Advances Research Project Agancy) Intuction Detection Dataset. [online] available: *http://kdd.ics.uci.edu/database/kddcup99/kddcup99.html*

[6] Tempo, 2017, "*Hacker merajalela di negara berkembang ada udang dibalik batu*", available [online] on *https://tekno.tempo.co/read/news/2017/07/05/072889051/hacker-merajalela-di-negara-berkembang-ada-udang-di-balik-batu* diakses tanggal 7 Juli 2017

[7] P Amudha, H Abdul Rauf. 2011. "*Performance Analysis of Data Mining Approaches in Intrusion Detection*". IEEE

[8] Khaerani Izza, Handoko Lekso Budi. 2015. "*Implementasi Dan Analisa Hasil Data Mining Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids) Dengan Algoritma C4.5*". Techno.com: Vol. 14 N0. 3 (181-188)

[9] Sundarajan N, Saratachandran, Wei Lu Ying. 1999. "*Radial Basis Function Neural Network with Sequential Learning*". World Scientific: Singapore

[10] Sutijo, Brodjol, Subanar, dan Suryo Guritno. "*Pemilihan Hubungan Input-Node Pada Jaringan Saraf*". Jurnal MIPA, 2006: 56-60.

[11] Jia Weikuan, Zhao Dean, Shen Tian, Su Chunyang, Chanli Hu, Zhao Yuyan. 2014. "*A New Optimized GA-RBF Neural Network Algorithm"*. Handawi Publishing Corporation Computational Intelligence and Neurosience: vol 2014, ID 982045

[11] Rajasekaran, S. 2007. "*Neural Networks, Fuzzy Logic, and Genetic Algorithms Synthesis and Applications*". Prentice-Hall of India Private Limited: New Delhi