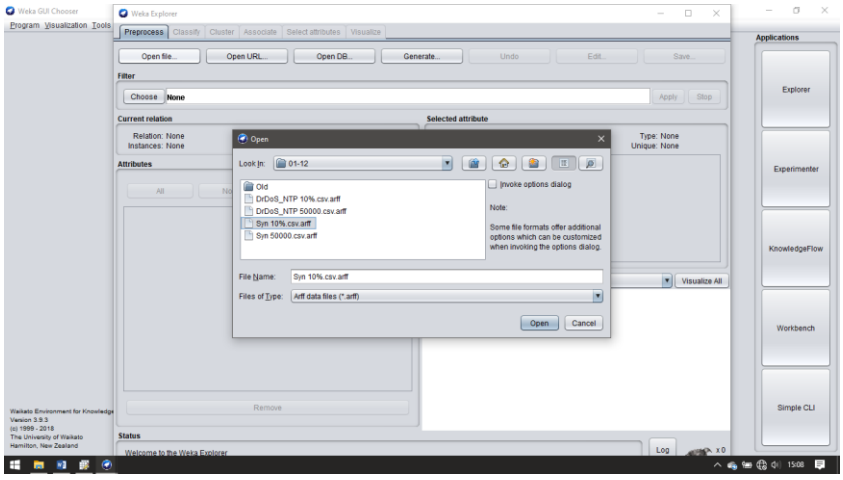
BAB IV
HASIL DAN PEMBAHASAN

Dalam penelitian ini, kedua serangan DDoS yang diantaranya Baik serangan SYN Flood (Berdasarkan Serangan TCP - Serangan Exploitasi), maupun serangan NTP (Berdasarkan Serangan UDP-Serangan Refleksi) terdapat 88 atribut didalamnya yang digunakan.

Proses klasifikasi pada *dataset* di penelitian ini dengan menggunakan program *data mining* WEKA untuk mengevaluasi model prediksi yang dibuat. Sebelum proses klasifikasi dilakukan, *dataset* serangan DDoS di-unggah kedalam program WEKA.



Gambar 4.1 Proses unggah *Dataset* serangan DDoS pada WEKA.

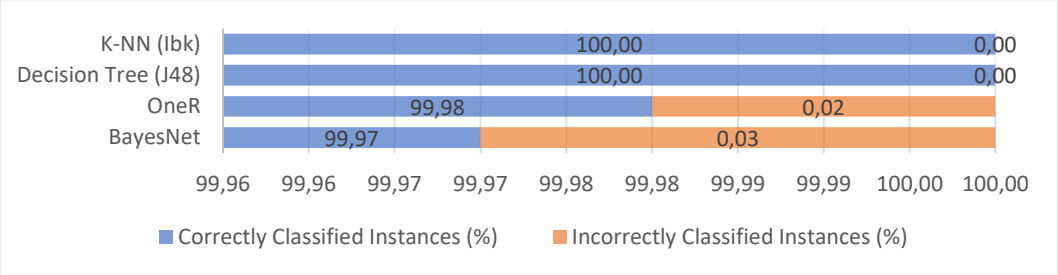
Baik serangan SYN Flood (Berdasarkan Serangan TCP - Serangan Exploitasi), maupun serangan NTP (Berdasarkan Serangan UDP - Serangan Refleksi) kedua serangan tersebut akan dilakukan proses klasifikasi dengan menggunakan algoritma *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48).* Menu *Test Option* adalah *Cross-Validation* dan mode tes yang digunakan adalah pengaturan *default.*

4.1. Klasifikasi *Correctly* dan *Incorrectly Instance*

Berdasarkan pengujian dengan menggunakan atribut yang ada pada *dataset* dapat di perlihatkan hasil *Correctly* dan *Incorrectly Instance* dengan menggunakan algoritma *Bayesian Network, IBk(K-NN), OneR, dan Decision Tree (J48)* dengan serangan SYN pada *dataset* DDoS yang akan di tampilkan pada tabel 4.1 dan gambar 4.2.

Tabel 4.1 Hasil Perbandingan *Correctly* dan *Incorrectly Instance* di Serangan SYN pada DDoS

	BayesNet	OneR	J48	IBk
Correctly Classified Instances (%)	99,97	99,98	100,00	100,00
Incorrectly Classified Instances (%)	0,03	0,02	0,00	0,00

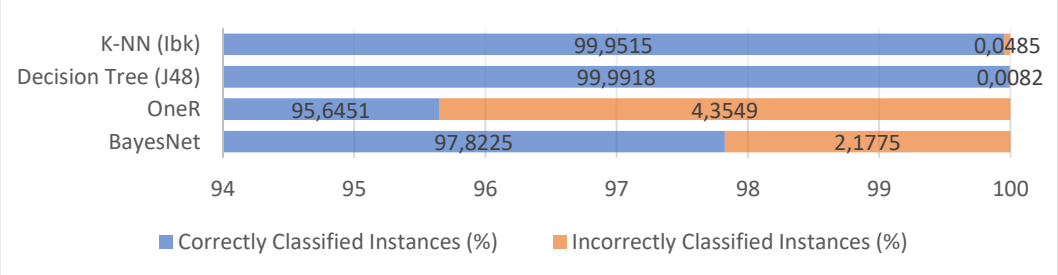


Gambar 4.2 Grafik Hasil Perbandingan *Correctly* dan *Incorrectly Instance* di Serangan SYN pada DDoS

Untuk hasil *Correctly* dan *Incorrectly Instance* dengan menggunakan algoritma tersebut dengan serangan NTP pada *dataset* DDoS yang akan di tampilkan pada tabel 4.2 dan gambar 4.3.

Tabel 4.2 Hasil Perbandingan *Correctly* dan *Incorrectly Instance* di Serangan NTP pada DDoS

	BayesNet	*OneR*	*J48*	*IBk*
Correctly Classified Instances (%)	97,8225	95,6451	99,9918	99,9515
Incorrectly Classified Instances (%)	2,1775	4,3549	0,0082	0,0485



Gambar 4.3 Grafik Hasil Perbandingan *Correctly* dan *Incorrectly Instance* di Serangan NTP pada DDoS

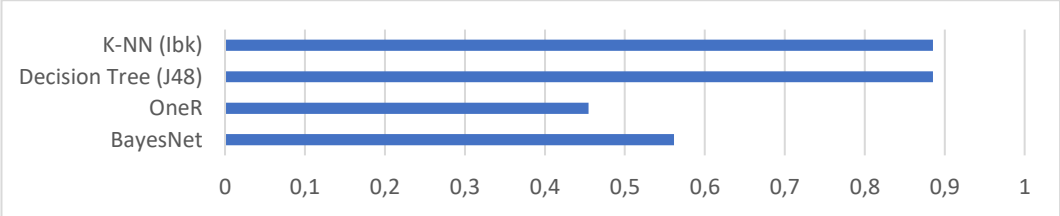
Dari hasil grafik perbandingan pada klasifikasi *Correctly* dan *Incorrectly Instance* pada serangan SYN, nilai tertinggi dicapai pada algoritma *Decision Tree (J48)* dan *K-NN (IBk)* dengan nilai keduanya 100,00 *Correctly Classified Instances (%)* dan nilai 0,00 *Incorrectly Classified Instances (%)*. Untuk serangan NTP, nilai tertinggi dicapai juga pada algoritma Decision Tree (J48) dengan nilai 99,9918 *Correctly Classified Instances (%)* dan nilai 0,0082 *Incorrectly Classified Instances (%).*

4.2. *Kappa Statistics*

Kappa mengacu pada ukuran yang diperbaiki secara kebetulan yang dihitung antara *Classification* dan *True Classes*. Ukuran tersebut dihitung dengan mengambil atribut yang diharapkan dari nilai atribut yang diamati. Nilai tersebut kemudian dibagi dengan nilai maksimum atribut. Nilai lebih besar dari nol menunjukkan kinerja yang lebih baik dibandingkan dengan peluang. Berikut adalah hasil *Kappa Statistic* dengan menggunakan algoritma *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48)* dengan serangan SYN pada DDoS yang akan ditampilkan pada tabel 4.3 dan gambar 4.4

Tabel 4.3 Hasil Perbandingan *Kappa Statistic* di Serangan SYN pada DDoS

	BayesNet	*OneR*	*J48*	*IBk*
Kappa statistic	0,5613	0,4545	0,8852	0,8852

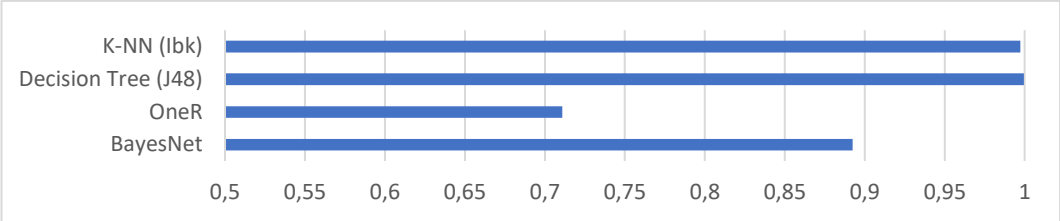


Gambar 4.4 Grafik Hasil *Kappa Statistic* di Serangan SYN pada DDoS

Untuk hasil *Kappa Statistic* menggunakan algoritma tersebut di serangan NTP pada *dataset* DDoS yang akan di tampilkan pada tabel 4.4 dan gambar 4.5.

Tabel 4.4 Hasil Perbandingan *Kappa Statistic* di Serangan SYN pada DDoS

	BayesNet	*OneR*	*J48*	*IBk*
Kappa statistic	0,8925	0,7109	0,9996	0,9974



Gambar 4.5 Grafik Hasil *Kappa Statistic* di Serangan NTP pada DDoS

Dari hasil grafik perbandingan pada klasifikasi *Kappa Statistic* pada serangan SYN, nilai tertinggi dicapai pada algoritma *Decision Tree (J48)* dan *K-NN (IBk)* dengan nilai keduanya 0,8852. Untuk serangan NTP, nilai tertinggi dicapai juga pada algoritma *Decision Tree (J48)* dengan nilai 0,9996.

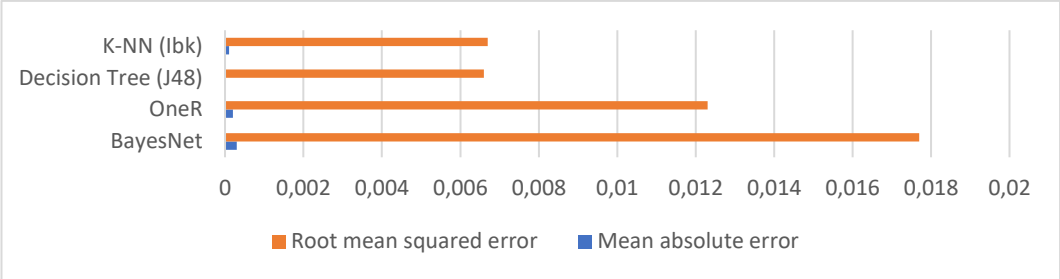
4.3. *Errors*

4.3.1. *Mean Absolute Error* (MAE) dan *Root Mean Squared Error* (RMSE)

Mean Absolute Error menghitung akurasi atribut yang memiliki variabel kontinu. Ini menghitung besarnya kesalahan rata-rata. Ini pada dasarnya adalah nilai rata-rata mutlak perbedaan antara pengamatan yang diprediksi dan pengamatan absolut. Akan tetapi, nilai rata-rata akar kuadrat juga menghitung besarnya kesalahan rata-rata tetapi perbedaannya terletak pada yang pertama dalam hal perbedaan antara pengamatan yang diprediksi dan pengamatan *absolute* yang dibagikan dan yang telah diputuskan dengan lebih dari pengamatan tersebut. Akar kuadrat dari rata-rata yang dihitung disebut sebagai RMSE. Nilai-nilai jenis kesalahan ini berkisar dari nol hingga tak terbatas. Dari diimplementasikan dengan *dataset* yang digunakan akan ditampikan nilai MAE dan RMSE pada serangan SYN dengan klasifikasi menggunakan *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48)* seperti pada tabel 4.5 dan gambar 4.6 berikut.

Tabel 4.5 Perbandingan *Mean Absolute Error* (MAE) dan *Root Mean Squared Error* (RMSE) di Serangan SYN pada *Dataset* DDoS

	BayesNet	*OneR*	*J48*	*IBk*
Mean absolute error	0,0003	0,0002	0	0,0001
Root mean squared error	0,0177	0,0123	0,0066	0,0067

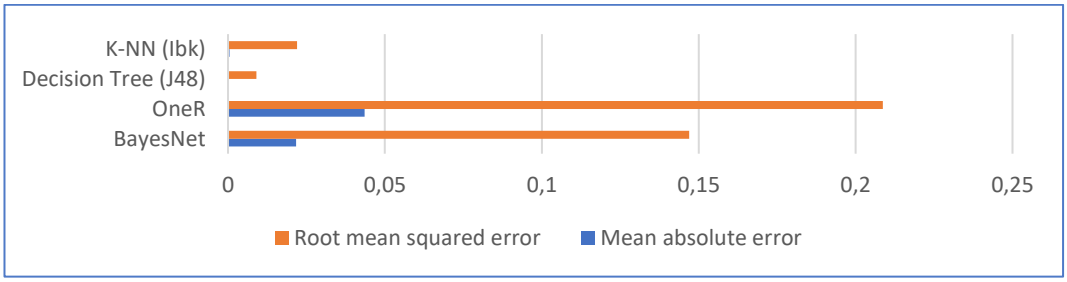


Gambar 4.6 Grafik Perbandingan Mean Absolute Error (MAE) dan Root Mean Squared Error (RMSE) di Serangan SYN pada *Dataset* DDoS

Untuk hasil MEA dan RSME menggunakan algoritma tersebut di serangan NTP pada d*ataset* DDoS yang akan di tampilkan pada tabel 4.6 dan gambar 4.7.

Tabel 4.6 Perbandingan Mean Absolute Error (MAE) dan Root Mean Squared Error (RMSE) di Serangan NTP pada *Dataset* DDoS

	BayesNet	*OneR*	*J48*	*IBk*
Mean absolute error	0,0217	0,0435	0,0001	0,0005
Root mean squared error	0,147	0,2087	0,009	0,022



Gambar 4.7 Grafik Perbandingan Mean Absolute Error (MAE) dan Root Mean Squared Error (RMSE) di Serangan NTP pada *Dataset* DDoS

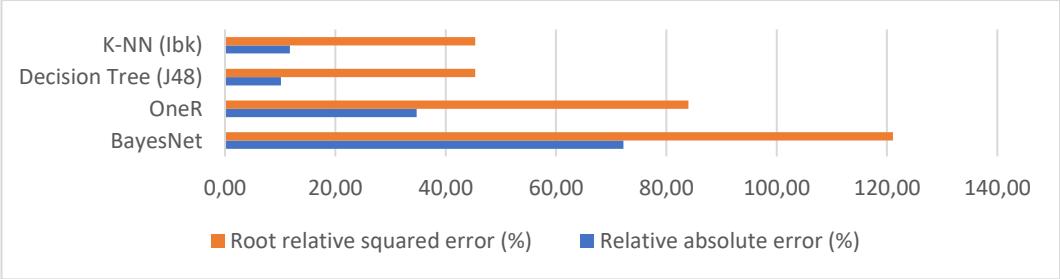
Dari hasil grafik perbandingan pada klasifikasi *Mean Absolute Error (MAE)* dan *Root Mean Squared Error (RMSE)* pada serangan SYN, nilai tertinggi dicapai pada algoritma *BayesNet* dengan nilai 0,0003 (MAE) dan 0,0177 (RMSE). Pada serangan NTP, nilai tertinggi dicapai juga pada algoritma *OneR* dengan nilai 0,0435 (MAE) dan 0,2087 (RMSE).

4.3.2. *Relative Absolute Error (RAE)* dan *Root Relative Squared Error (RRSE)*

Berikut ini adalah kesalahan (*error*) yang membuat kinerja setiap percobaan dihitung. Kesalahan *absolute* memberikan jumlah kesalahan fisik, sedangkan kesalahan relatif memberikan informasi tentang seberapa efisien pengukuran tertentu relatif terhadap ukuran atribut yang diukur. Dengan *dataset* yang diambil dalam percobaan ini, akan ditampilkan hasil dari RAE dan RRSE pada serangan SYN dengan klasifikasi menggunakan *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48)* seperti pada tabel 4.7 dan gambar 4.8 berikut.

Tabel 4.7 Perbandingan Hasil RAE dan RRSE pada Serangan SYN

	BayesNet	*OneR*	*J48*	*IBk*
Relative absolute error (%)	72,25	34,7345	10,1296	11,7388
Root relative squared error (%)	121,09	84,0258	45,3735	45,3788

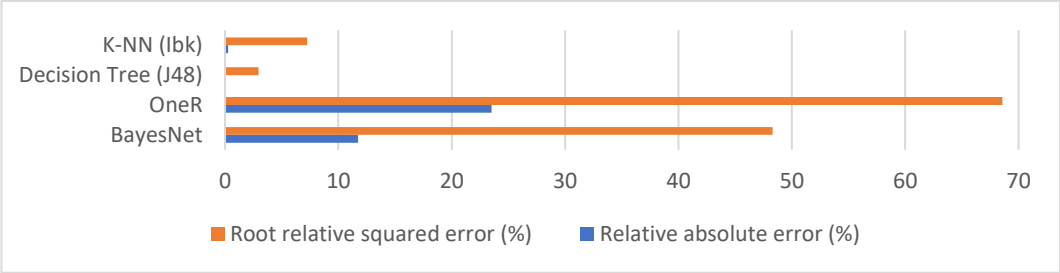


Gambar 4.8 Grafik Perbandingan Hasil RAE dan RRSE pada Serangan SYN

Untuk hasil RAE dan RRSE menggunakan algoritma tersebut di serangan NTP pada *dataset* DDoS yang akan di tampilkan pada tabel 4.8 dan gambar 4.9.

Tabel 4.8 Perbandingan Hasil RAE dan RRSE pada Serangan NTP

	BayesNet	*OneR*	*J48*	*IBk*
Relative absolute error (%)	11,7344	23,5161	0,0487	0,2667
Root relative squared error (%)	48,3151	68,5811	2,9672	7,2358



Gambar 4.9 Grafik Perbandingan Hasil RAE dan RRSE pada Serangan NTP

Dari hasil grafik perbandingan pada klasifikasi *Relative Absolute Error (RAE)* dan *Root Relative Squared Error (RRSE)* pada serangan SYN, nilai tertinggi dicapai pada algoritma *OneR* dengan nilai 39,2976 (RAE) dan 89,4695(RRSE). Untuk serangan NTP, nilai tertinggi dicapai juga pada algoritma *Decision Tree (J48)* dengan nilai 27,828 (RAE) dan 74,6036 (RRSE).

4.4. *Accuracy Measurement*

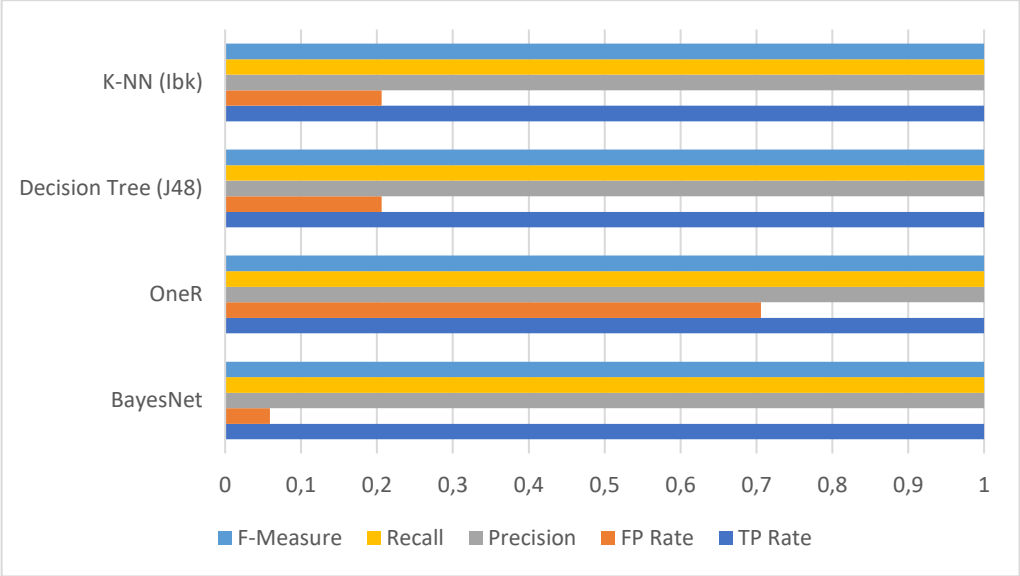
Keakuratan algoritma diukur dengan bantuan parameter seperti laju TP, laju FP, presisi, daya ingat dan pengukuran-F. Parameter-parameter ini didefinisikan ulang sebagai berikut:

a. TP Rate: Dikenal sebagai tingkat True Positive. Ini mendefinisikan instance yang telah diklasifikasikan dengan benar sehubungan dengan kelas yang diberikan.
b. FP Rate: Dikenal sebagai tingkat False Positive. Ini mendefinisikan instance yang telah secara salah atau salah diklasifikasikan sehubungan dengan kelas vektor.
c. Precision: Ini mencantumkan proporsi instance yang benar untuk kelas tertentu dibagi dengan instance keseluruhan yang diklasifikasikan sehubungan dengan kelas itu.
d. Recall: Ini menentukan proporsi instance yang telah diklasifikasikan oleh kelas dibagi dengan total instance yang ada di kelas.
e. F-Measure: Dihitung dengan menggabungkan ukuran Recall dan Precision.

Berikut adalah nilai dari *TP Rate, FP Rate, Precision, Recall, F-Measure* dari serangan SYN dengan klasifikasi menggunakan *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48)* akan di tampilkan pada tabel 4.9 dan gambar 4.10.

Tabel 4.9 Hasil Nilai TP Rate, FP Rate, Precision, Recall, F-Measure pada Serangan SYN

	BayesNet	*OneR*	*J48*	*IBk*
TP Rate	1	1	1	1
FP Rate	0,059	0,706	0,206	0,206
Precision	1	1	1	1
Recall	1	1	1	1
F-Measure	1	1	1	1

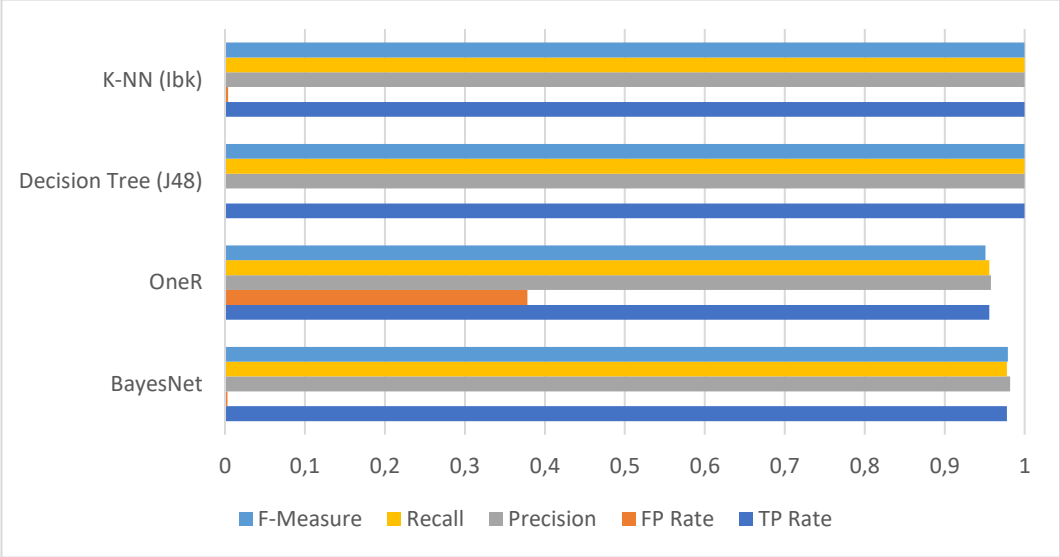


Gambar 4.10 Grafik Hasil Nilai *TP Rate, FP Rate, Precision, Recall, F-Measure* pada Serangan SYN

Untuk hasil *TP Rate, FP Rate, Precision, Recall, F-Measure* menggunakan algoritma tersebut di serangan NTP pada *Dataset* DDoS yang akan di tampilkan pada tabel 4.10 dan gambar 4.11.

Tabel 4.10. Hasil Nilai *TP Rate, FP Rate, Precision, Recall, F-Measure* pada Serangan NTP

	BayesNet	*OneR*	*J48*	*IBk*
TP Rate	0,978	0,956	1	1
FP Rate	0,003	0,378	0	0,004
Precision	0,982	0,958	1	1
Recall	0,978	0,956	1	1
F-Measure	0,979	0,951	1	1



Gambar 4.11 Grafik Hasil Nilai *TP Rate, FP Rate, Precision, Recall, F-Measure* pada Serangan NTP

Berikut akan di tampilkan pada Tabel 4.11 untuk contoh klasifikasi *confusion matrix* yang akan disajikan.

Tabel 4.11. *Confusion Matrix*

	Correctly Classified	*Incorrectly Classified*
Selected	TP	FP
Not Selected	FN	TN

Berikut adalah hasil dari *Confusion Matrix* dari serangan SYN pada hasil klasifikasi menggunakan algoritma *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48).*

Tabel 4.12 *Confusion Matrix* Serangan SYN Flood dengan Algoritma *Bayesian Network*

a	*b*	*<-- classified as*
158188	48	*a = Syn*
2	32	*b = BENIGN*

Tabel 4.13 *Confusion Matrix* Serangan SYN Flood dengan Algoritma *OneR*

a	*b*	*<-- classified as*
158236	0	*a = Syn*
24	10	*b = BENIGN*

Tabel 4.14 *Confusion Matrix* Serangan SYN Flood dengan Algoritma *Decision Tree (J48)*

a	*b*	*<-- classified as*
158236	0	*a = Syn*
7	27	*b = BENIGN*

Tabel 4.15 *Confusion Matrix* Serangan SYN Flood dengan Algoritma *K-NN(IBk)*

a	*b*	*<-- classified as*
158236	0	*a = Syn*
7	27	*b = BENIGN*

Berikut adalah hasil dari *Confusion Matrix* dari serangan NTP pada hasil klasifikasi menggunakan algoritma *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48).*

Tabel 4.16 *Confusion Matrix* Serangan NTP dengan Algoritma *Bayesian Network*

a	*b*	*<-- classified as*
106485	2650	*a = DrDoS_NTP*
0	12566	*b = BENIGN*

Tabel 4.17 *Confusion Matrix* Serangan NTP dengan Algoritma *OneR*

a	*b*	<-- *classified as*
109135	0	*a = DrDoS_NTP*
5300	7266	*b = BENIGN*

Tabel 4.18 *Confusion Matrix* Serangan NTP dengan Algoritma *Decision Tree (J48)*

a	*b*	<-- *classified as*
109130	5	*a = DrDoS_NTP*
5	12561	*b = BENIGN*

Tabel 4.19 *Confusion Matrix* Serangan NTP dengan Algoritma *K-NN (IBk)*

a	*b*	<-- *classified as*
109135	0	*a = DrDoS_NTP*
59	12507	*b = BENIGN*

Setelah mendapati nilai *Confusion Matrix* dari kedua serangan, baik serangan SYN maupun serangan NTP, selanjutnya menghitung nilai *Sensitivity*, *Specificity*, *Accuracy* dan *F-measure*. Nilai *Sensitivity*, *Specificity* , *Accuracy* dan *F-measure* dapat dihitung dengan rumus berikut:

$$Specificity = \frac{TN}{TN+FP} \quad (6)$$

$$Sensitivity = \frac{TP}{TP+FN} \quad (7)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FN+FP} \quad (8)$$

$$F-measure = 2\,\frac{SP*SN}{SP+SN} \quad (9)$$

Dimana,

TP = True Positive, FP = False Positive,

TN = True Negative, FN = False Negative.

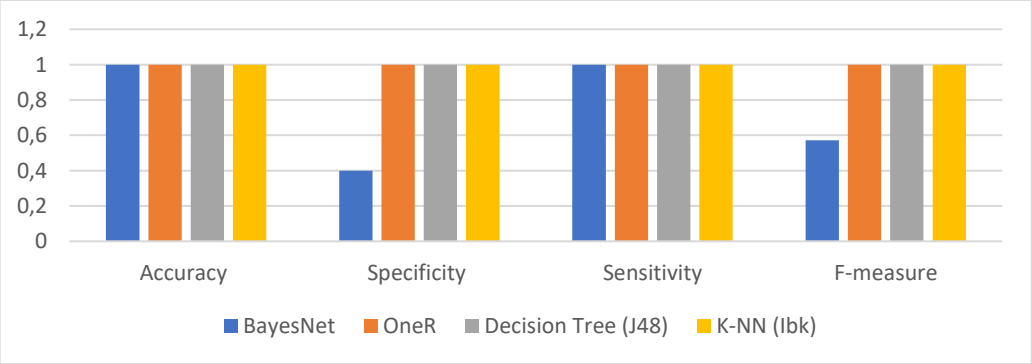
Accuracy merupakan sebuah pengujian untuk mencari tahu kemampuan dari algoritma dalam membedakan hasil serangan SYN dan NTP baik yang benar serangan maupun yang bukan serangan (traffic normal / *benign*) secara

keseluruhan. *Specificity* merupalam pengujian untuk mencari tahu kemampuan dari model yang dikembangkan dalam menentukan *instans* yang akan diklasifikasikan benar dengan jumlah total instans dalam data. Sensitivity merupakan nilai yang menyatakan *rasio instans* positif yang diklasifikasikan benar terhadap semua instans dalam kelas aktual. Sementara metrik *F-measure* adalah untuk menghitung nilai *mean* yang merupakan gabungan dari *Sensitivity* dan *Specificity*

Dengan menggunakan rumus ini, akan didapati *Sensitivity*, *Specificity* , *Accuracy* dan *F-measure* untuk algoritma yang digunakan, lalu membandingkan untuk memeriksa mana yang memberikan hasil lebih baik. Berikut adalah hasil nilai *Sensitivity*, *Specificity*, *Accuracy* dan *F-measure* dari serangan SYN pada hasil klasifikasi menggunakan algoritma *Bayesian Network, IBK(K-NN), OneR,* dan *Decision Tree (J48)* yang akan di tampikan pada tabel 4.20 dan gambar 4.12.

Tabel 4.20 Hasil *Sensitivity*, *Specificity*, *Accuracy* dan *F-measure* pada Serangan SYN

	BayesNet	OneR	J48	IBk
Accuracy	0,999684084	0,99984836	0,999955772	0,99995577
Specificity	0,4	1	1	1
Sensitivity	0,999987357	0,999848351	0,999955764	0,99995576
F-measure	0,571426507	0,99992417	0,999977882	0,999977882



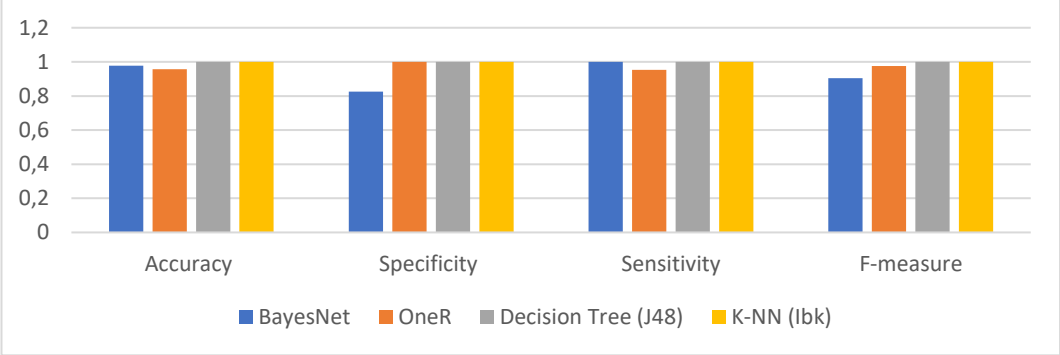
Gambar 4.12 Grafik Hasil *Sensitivity*, *Specificity*, *Accuracy* dan *F-measure* pada Serangan SYN

Berikut juga adalah hasil nilai *Sensitivity, Specificity* , *Accuracy* dan *F-measure* dari serangan NTP pada hasil klasifikasi menggunakan algoritma *Bayesian Network,*

IBK(K-NN), OneR, dan *Decision Tree (J48)* yang akan di tampikan pada tabel 4.21 dan gambar 4.13.

Tabel 4.21 Hasil *Sensitivity*, *Specificity*, *Accuracy* dan *F-measure* pada Serangan NTP

	BayesNet	OneR	J48	IBk
Accuracy	0,978225323	0,956450645	0,999917831	0,999515205
Specificity	0,82584122	1	0,999602101	1
Sensitivity	1	0,953685498	0,999954185	0,999459677
F-measure	0,904614499	0,976293778	0,999778112	0,999729765



Gambar 4.13 Grafik Hasil *Sensitivity*, *Specificity*, *Accuracy* dan *F-measure* pada Serangan NTP

Dari hasil grafik pada serangan SYN, nilai tertinggi (*Accuracy*) dicapai pada algoritma Decision Tree (J48) dengan nilai 0,999955772. Untuk nilai tertinggi (*Specificity*) dicapai pada algoritma OneR, dan K-NN(Ibk) yang juga mendapatkan nilai 1,0. Untuk nilai tertinggi (*Sensitivity*) dicapai pada algoritma BayesNet dengan nilai 0,999987357. Untuk nilai tertinggi (*F-measure*) dicapai pada algoritma OneR, dan K-NN(Ibk) dengan nilai keduanya 0,999977882.

Selanjutnya, pada serangan NTP, nilai tertinggi (*Accuracy*) dicapai pada algoritma Decision Tree (J48) dengan nilai 0,999917831. Untuk nilai tertinggi (*Specificity*) dicapai pada algoritma OneR dan K-NN (Ibk) yang mendapatkan nilai 1,0. Untuk nilai tertinggi (*Sensitivity*) dicapai pada algoritma BayesNet dengan nilai 1,0. Untuk nilai tertinggi (*F-measure*) dicapai pada algoritma Decision Tree (J48) dengan nilai 0,999778112.