Klasifikasi Dokumen berkonten Serangan jaringan menggunakan Multinomial Naive Bayes

Bambang Harjito1, Kuni Nur Aini2, Budi Murtiyasa3
[1,2] Department of Informatics, Faculty of Mathematics and Natural Science,
Universitas Sebelas Maret, Jln. Ir. Sutami No. 36 A Kentingan Surakarta Indonesia
[3] Universitas Muhammadiyah Surakarta
bambang_harjito@staff.uns.ac.id , kuninuraini@student.uns.ac.id, budi.murtiyasa@ums.ac.id

Abstrak – Kebutuhan konsumen akan informasi dalam bentuk jurnal atau artikel semakin meningkat, sehingga diperlukan pengelompokan jurnal untuk memfasilitasi pengambilan informasi. Salah satu metodenya adalah Multinomial Naïve Bayes (MNB) yang digunakan untuk mengatur sejumlah besar informasi. MNB mudah digunakan untuk melakukan klasifikasi dokumen. MNB mengidentifikasi objek kelas yang tidak diketahui dari proses pembelajaran. Tujuan dari makalah ini mengkategorikan dokumen bahasa Inggris yang terkait dengan "Serangan Jaringan" menggunakan Multinomial Naïve Bayes (MNB) dan Term Frequency-Inverse Document Frequency (TF-IDF). Hasil percobaan menunjukkan bahwa MNB dengan TF-IDF mendapatkan akurasi 76,00%. Dalam percobaan ini juga dihitung nilai presisi, recall, dan skor F1. Nilai Precession adalah 0,77, nilai Recall adalah 0,76 dan nilai Skor F1 adalah 0,76 masing-masing. Nilai-nilai ini digunakan untuk menentukan tingkat akurasi dari hasil yang diprediksi

1 Pendahuluan

Kebutuhan penguna terhadap informasi dalam bentuk jurnal atau artikel semakin meningkat, sehingga pengelompokan jurnal sangat dibutuhkan untuk mempermudah pencarian informasi. lnformasi penting dari jurnal berupa topic akan memberikan gambaran pokok pembahasan secara umum [1]. Artikel ilmiah merupakan ringkasan dari laporan penelitian yang biasanya dimuat di dalam jurnal-jurnal penelitian. Jurnal berisi suatu kutipan dari laporan yang menjadi point-point penting terkait topik tertentu, sehingga menjadi sumber pengetahuan bagi pembaca [2]. Pembahasan dalam jurnal meliputi berbagai bidang, salah satunya adalah bidang Information Technology (IT).

Permasalahan yang sering terjadi dalam bidang IT, misalnya terkait dengan keamanan jaringan. Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang dalam dunia IT. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep terbuka sistemnya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses suatu sistem. Namun hal tersebut juga memberikan dampak negatif, yaitu membuka peluang bagi seseorang yang tidak mempunyai akses untuk mencuri informasi, merusak sistem atau jaringan, melakukan manipulasi sistem dengan cara melakukan serangan pada jaringan atau sistem tertentu, permasalahan seperti ini biasa disebut dengan “Network attacks” [3].

Dengan banyaknya jurnal-jurnal yang membahas terkait “Serangan jaringan” (Network Attacks), memungkinkan sistem dapat mengelompokan jurnal-jurnal tersebut ke dalam masing-masing kategori attack. Pengelompokan dokumen bisa dilakukan dengan berbagai teknik, salah satunya adalah Text Mining. Text Mining adalah salah satu bidang khusus dari Data Mining yang merupakan suatu proses menggali informasi

dimana seorang user berinteraksi dengan sekumpulan dokumen menggunakan tools analisis, salah satuya adalah melakukan kategorisasi atau klasifikasi [4]. Salah satu metode yang digunakan untuk melakukan klasifikasi adalah Multinomial Naive Bayes.

Penelitian menunjukan bahwa metode Naive Bayes bekerja dengan baik untuk klasifikasi teks berita dan abstrak akademis, hasil akurasi maksimal pada dokumen berita sebesar 91% sedangkan pada dokumen akademik 82% [5].. Pada makalah ini dilakukan untuk mengkategorikan dokumen jurnal berbasis judul, abstrak dan kata kunci dengan cara klasifikasi menggunakan MNB. Penambahan fitur ekstraksi dilakukan untuk memilih beberapa fitur yang digunakan untuk mewakili dokumen, karena pada proses kategorisasi sering ditemukan masalah terkait tingginya dimensi data [6].

2. Text Mining, text processing and Term Frequncy – Inverse Document Frequency (TF-IDF)

Text mining juga disebut sebagai Teks Data Mining (TDM) atau Knowledge Discovery in Text (KDT), secara umum mengacu pada proses ekstraksi informasi dari dokumen-dokumen teks tak terstruktur (unstructured). Tujuan utama text mining adalah mendukung proses knowledge discovery pada koleksi dokumen yang besar. Text mining mencoba memecahkan masalah information overload dengan menggunakan teknik-teknik dari bidang ilmu yang terkait [7]. Sedangkan Text Processing adalah tahap melakukan analisis kebenaran arti (semantik) dan kebenaran susunan (sintaktik) terhadap teks. Tujuan dari pemrosesan awal adalah untuk mempersiapkan teks menjadi data yang akan mengalami pengolahan lebih lanjut. Tahapan-tahapan text preprocessing yaitu [7]; (a) Case folding. (b) Tokenizing, (c) Filtering dan (d) Tahap stemming.

Metode TF-IDF merupakan metode untuk menghitung bobot setiap kata yang paling umum digunakan pada information retrieval. Metode ini juga terkenal efisien, mudah dan memiliki hasil yang akurat [8]. Metode ini akan menghitung nilai Term Frequency (TF) dan Inverse Document Frequency (IDF) pada setiap token (kata) di setiap dokumen dalam korpus. Metode ini akan menghitung bobot setiap *token* t di dokumen d dengan rumus:

$$Wdt = tf(t,d) \times IDF(t) \quad (1)$$

d = dokumen ke-d, *t* = kata ke-t dari kata kunci, *W* = bobot dokumen ke-d terhadap kata ke-t , t*f* = banyaknya kata yang dicari pada sebuah dokumen, *IDF* :Inversed Document Frequency. Nilai *IDF* didapatkan dari

$$IDF(t) : log\ (D/df) \quad (2)$$

D = total dokumen, *df*= banyak dokumen yang mengandung kata yang dicari. Setelah bobot *(W)* masing-masing dokumen diketahui, maka dilakukan proses pengurutan dimana semakin besar nilai *W*, semakin besar tingkat similaritas dokumen tersebut terhadap kata kunci, demikian sebaliknya

3. Multinomial Naive Bayes (MNB)

MNB merupakan salah satu metode spesifik dari Naive Bayes. Metoda ini secara umum merupakan probabilitas suatu dokumen, sebagai bagian dari anggota kelas C [9]. Persamaan 1 probabilitas dari suatu dokumen d terhadap kelas C dapat dihitung dengan rumus sebagai berikut:

$$P(C|term\ dokumen\ d) = P(X_1|C) \times P(X_2|C) \times \ldots \times P(X_n|C) \times P(C) \quad (3)$$

P(C)= Probabilitas prior dari kelas C, X_n= Kata dokumen d ke-n, *P(C|term dokumen)* = Probabilitas suatu dokumen termasuk kelas C , $P(X_n|C)$= Probabilitas kata ke-n dengan diketahui kelas C.

Probabilitas prior kelas c ditentukan dengan rumus:

$$P(C) = \frac{N_c}{N} \quad (4)$$

Nc= Jumlah kelas C pada seluruh dokumen, *N*= Jumlah seluruh dokumen, Probabilitas kata ke-n ditentukan dengan menggunakan persamaan sebagai berikut:

$$P(X_n|C) = \frac{N_{x_n,c} + \alpha}{N(C)+V} \quad n = (1, \dots, n) \quad (5)$$

$N_{x_n,c}$= Jumlah term X_n yang ditemukan di seluruh data pelatihan dengan kategori C

N(C)= Jumlah term di seluruh data pelatihan dengan kategori C, α= Parameter *laplace smoothing* , *V*= Jumlah seluruh kata pada data pelatihan

Sementara rumus Multinomial yang digunakan dengan pembobotan TF-IDF adalag sebagai berikut :

$$P(X_n|C) = \frac{\sum tf(X_n, d\epsilon C)+\alpha}{\sum N_{d\epsilon C}+V} \quad (6)$$

$\sum tf(X_n, d\epsilon C)$ = Jumlah pembobotan kata X_n dari seluruh dokumen pada *training sample* pada kategori C $\sum N_{d\epsilon C}$ = Jumlah bobot seluruh *term* pada data *training* dari kategori C.

4. Klasifikasi dokumen "Networks Attack" menggunakan MNB

4.1 Data dan evaluasi yang digunakan

Data yang digunakan dalam penelitian ini berjumlah 1000 jurnal dengan konten "Network Attacks" dari laman ieeexplore.ieee.org www.sciencedirect.com dari tahun 2014-201, sebagai sumber data utama dan sejumlah website lainnya sebagai sumber pelengkap. Pengambilan data dilakukan pada bulan September 2017 (Tabel 1).

Tabel 1 Data 1000 Jurnal yang terkategorikan

Kategori	Tahun				**Jumlah**
	2014	2015	2016	2017	
DOS	42	45	63	37	**187**
General	31	47	32	34	**144**
Malicious software	29	42	42	42	**155**
Man in the middle	38	23	42	23	**126**
Password attack	34	38	33	28	**133**
Phishing	27	36	36	33	**132**
Spoofing	31	33	33	30	**123**
Jumlah	232	260	281	227	

Proses Evaluasi pada makalah ini menggunakan perhitungan *precision*, *recall*, dan *f1-score* dari hasil klasifikasi yang disajikan dengan rumus perhitungan sebagai berikut:

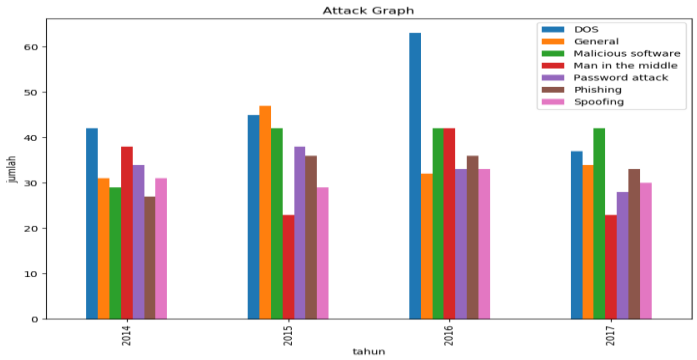
$precision = \frac{TP(Kelas-i)}{Prediksi(Kelas-i)}$, $recall = \frac{TP(Kelas-i)}{Total(Kelas-i)}$, $F1 - Score = \frac{2\ x\ Precision\ x\ Recall}{Precision+Recall}$ dan

$Accuracy = \frac{\text{TP(Kelas}-1)+ \text{TP(Kelas}-2)+..+\text{TP(Kelas}-n)}{Total\ (Kelas-1)+Total(Kelas-2)+\cdots+Total(Kelas-n)}\ x\ 100\%$

TP = *True Positive*, TN= *True Negative*, FP = *False Positive*, FN= *False Negative*

4.2 Klasifikasi menggunakan Multinomial Naïve Bayes

Data yang digunakan telah dijelaskan pada sub bagian 4.1, selanjutnya kelompokkan menjadi 7 kategori secara manual. Pembagian data ke dalam 7 kategori akan ditampilkan dalam bentuk grafik yang dapat dilihat pada Gambar 1.



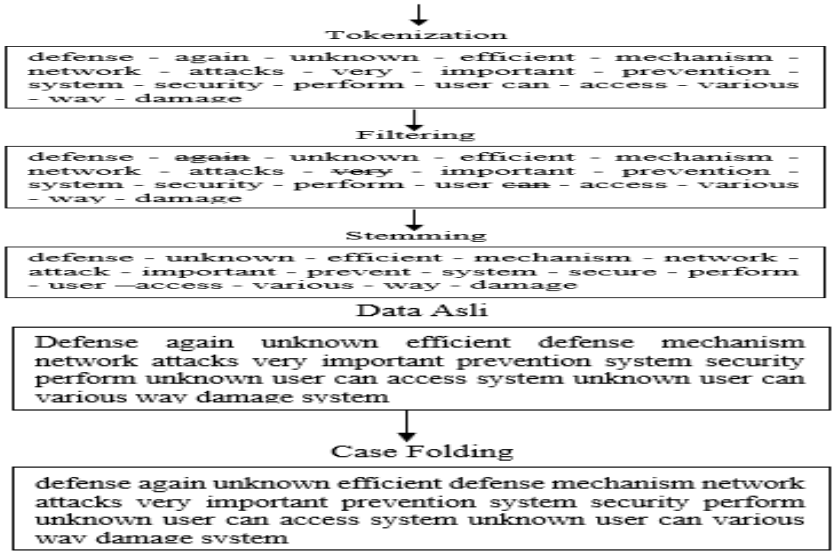
Gambar 1 Hasil running Grafik Jenis Serangan

Dalam penyajian grafik diatas hanya menggunakan data tahun dan kategori**.** Pada proses klasifikasi data tersebut akan dibagi ke dalam dua proses yaitu training dan testing. Data yang digunakan pada proses training sejumlah 700 sedangkan pada proses testing sejumlah 300 data. Berikut ini adalah tahapan klasifikasi

4.2.1 Tahapan Text Processing

Dalam proses *text processing* terdapat empat tahapan. Tahap pertama yaitu *case folding* yang bertujuan untuk menghilangkan semua karakter selain huruf di dalam data dan mengubah semua huruf menjadi huruf kecil. Tahap kedua yaitu *tokenization* yang bertujuan untuk mengubah bentuk *string* menjadi *token* atau kata.

Tahap selanjutnya adalah *filtering* yang bertujuan untuk menghilangkan *stopwords*. Kemudian tahap terakhir adalah *stemming* yaitu semua kata diproses untuk menghilangkan imbuhan pada kata tersebut, sehingga semua kata menjadi kata dasar atau *root word*, proses *stemming* dilakukan menggunakan *library Porter Stemmer*. Contoh tahapan *text processing* ditunjukkan pada Gambar 3 berikut ini.



Gambar 3 Contoh Text Processing

4.2.2 Pembobotan TF-IDF

Proses pembobotan *TF-IDF* ini dimulai dengan menghitung tiap *term* yang ada pada setiap dokumen *(TF)*. Kemudian proses dilanjutkan dengan menghitung jumlah dokumen yang mempunyai *term* tertentu *(DF)*. Setelah itu proses menghitung *Inverse Document Frequency (IDF)* dan yang terakhir nilai *TF* dikalikan dengan *IDF*.
Misalnya terdapat 5 dokumen yang akan digunakan sebagai pedoman dalam perhitungan *TF-IDF*

- Dokumen ke 1 (D1) =

defense *again* ***unknown*** *efficient* ***defense*** *mechanism network* ***attack*** *very important prevention system security perform* ***unknown user*** *can access system* ***unknown user*** *can various way damage system*

- Dokumen ke 2 (D2) =

literature survey social engineer ***attack phishing attack phishing*** *network type* ***attack attack*** *create fake existing webpage prime objective review do literature survey social engineering* ***attack unknown*** *person can access system use various* ***trick***

- Dokumen ke 3 (D3) =

performance analysis dos land ***attack*** *detection use* ***trick*** *detection prevention dos* ***attack*** *use* ***method****. kind* ***attack*** *which phisher* ***unknown*** *use spoof email and fraudulent web sites* ***trick*** *people*

- Dokumen ke 4 (D4) =

spear ***phishing attack*** *get stead sophisticat cyber criminal use social engineering* ***trick*** *denizen internet come barrage* ***phishing attack*** *increase frequency and sophistic* ***method*** *blacklist* ***phishing*** *website* ***phishing*** *continue unabate plague internet* ***unknown*** *person* ***trick*** *provide personal confident* ***trick*** *infromation* ***trick*** *can use to prevent* ***phishing*** *from* ***unknown*** *person but somene can has.*

- Dokumen ke 5 (D5) =

method trick unknown *provide personal finance information effective* ***defense*** *scheme mobile compute platforms penetration testing concepts* ***defense*** *strategies*

Ke lima 5 dokumen di atas hanya beberapa kata yang akan digunakan untuk mewakili contoh perhitungan *TF-IDF*, yaitu kata**: *phishing, attack, defense, method, trick, user, unknown.***
Perhitungan TF-IDF ditampilkan pada tabel 3 berikut ini.

Tabel 3 Contoh Perhitungan TF-IDF

	TF						TF-IDF				
Kata	D1	D2	D3	D4	D5	IDF	D1	D2	D3	D4	D5
phishing	0	2	0	5	0	0,40	0,00	0,80	0,00	1,99	0,00
attack	1	5	3	2	0	0,10	0,10	0,48	0,29	0,19	0,00
defense	2	0	0	0	2	0,40	0,80	0,00	0,00	0,00	0,80
method	0	0	1	1	1	0,22	0,00	0,00	0,22	0,22	0,22
trick	0	1	2	3	1	0,10	0,00	0,10	0,19	0,29	0,10
user	2	0	0	0	0	0,70	1,40	0,00	0,00	0,00	0,00
unknow	3	1	1	2	1	0,00	0,00	0,00	0,00	0,00	0,00

4.2.3 Klasifikasi

Data yang telah dilakukan training menggunakan TF-IDF kemudian dijadikan sebagai bahan pembelajaran pada proses testing untuk menentukan suatu data jurnal masuk ke dalam kelas tertentu. Data yang menjadi testing set melalui proses klasifikasi dengan menggunakan metode MNB. Tahapan proses klasifikasi berdasarkan Tabel 4:

Tabel 4 Perhitungan Klasifikasi

	tf						tf-idf				
term	D1	D2	D3	D4	D5	idf	D1	D2	D3	D4	D5
phishing	0	2	0	5	0	0,40	0,00	0,80	0,00	1,99	0,00
attack	1	5	3	2	0	0,10	0,10	0,48	0,29	0,19	0,00
defense	2	0	0	0	2	0,40	0,80	0,00	0,00	0,00	0,80
method	0	0	1	1	1	0,22	0,00	0,00	0,22	0,22	0,22
trick	0	1	2	3	1	0,10	0,00	0,10	0,19	0,29	0,10
user	2	0	0	0	0	0,70	1,40	0,00	0,00	0,00	0,00
unknown	3	1	1	2	1	0,00	0,00	0,00	0,00	0,00	0,00
Class							probing	phishing	probing	phishing	probing
Jumlah							2,29	1,38	0,71	2,70	1,11

4.2.4. Evaluasi Data Testing

Data yang digunakan sebagai testing set adalah 300 data dari 1000 data. Artinya 30% dari jumlah data. Hasil evaluasi seluruh data testing dilakukan sebagai berikut ini.

- MNB menggunakan TF-IDF

Klasifkasi menggunakan *MNB* disertai *TF-IDF* dimulai dengan menginputkan *data set* dengan format csv, kemudian dilakukan perhitungan bobot setiap kata menggunakan *TF-IDF* (berlaku persamaan 1), selanjutnya proses klasifikasi menggunakan *MNB* (berlaku persamaan 3). Hasilnya adalah nilai *accuracy* untuk mengetahui tingkat kebenaran hasil prediksi ynag dapat dilihat dalam Tabel 5.

Tabel 5 Evaluasi Metode MNB (TF-DF)

Metode	Accuracy (%)
MNB	76.00

Accuracy adalah pembagian dari jumlah data yang diklasifikasikan dengan benar dibagi dengan total data *testing.* Untuk metode MNB diketahui bahwa jumlah data yang diklasifikasin dengan benar adalah 227 data kemudian dibagi dengan 300, sehingga dihasilkan akurasi yaitu 76,00 %.

- MNB (TF-IDF) menggunakan *precision, recall, dan f1-score.*

Menggunakan persamaan 3*, didapatkan* nilai *precision, recall, f1-score* untuk mengetahui tingkat kebenaran hasil prediksi yang dapat dilihat dalam Tabel 6

Tabel 6 Evaluasi dengan Precision, Recall, F1-Score (TFIDF- Count Vector)

Metode	Precision	Recall	F1-Score
MNB-TFIDF	0.77	0.76	0.76

5. Kesimpulan

Dalam makalah ini telah berhasil dilakukan klasfikasi dokumen jurnal yang membahas terkait "Networks Attaks " dengan menggunakan metoda MNB. Penggunaan metode MNB disertai TF-IDF cukup baik dalam mengklasifikasi dokumen dengan akurasi sebesar 76.00%. Perhitungan metoda MNB (TF-IDF) menggunakan precision, recall, dan f1-score didapatkan nilai Precesion sebesar 0,77, nilai Recall sebesar 0,76 dan nilai F1 Score sebesar 0,76. Hasil nilai-nilai nilai precision, recall, f1-score diguankan untuk mengetahui tingkat kebenaran hasil prediksi. Pengembangan penelitian selanjutnya dapat dilakukan dengan membandingkan dengan metode lain seperti K-Nearest Neighbors method (KNN), Support Vector Machine Linear (SVM Linear), Random Forest.

References

1. Indranandita, A., B. Susanto, and A. Rahmat, *Sistem Klasifikasi dan Pencarian Jurnal dengan Menggunakan Metode Naive Bayes dan Vector Space Model*. Jurnal Informatika, 2011. **4**(2).
2. Budiyanto, D., *Mengenal Karya Ilmiah.* Jurnal, 2012.
3. Wajong, A.M., *Kerentanan yang Dapat Terjadi di Jaringan Komputer pada Umumnya.* ComTech: Computer, Mathematics and Engineering Applications, 2012. 3(1): p. 474-481.
4. Triawati, C., *Text Mining.* Retrieved October, 2009. 27: p. 2016.
5. Hamzah, A. *Klasifikasi teks dengan naïve bayes classifier (nbc) untuk pengelompokan teks berita dan abstract akademis*. in *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) Periode III*. 2012.
6. StatSoft. *Text Mining Introductory Overview*. 2016.
7. Nugroho, E., *Perancangan Sistem Deteksi Plagiarisme Dokumen Teks Dengan Menggunakan Algoritma Rabin-Karp.* Jurusan Ilmu Komputer, Universitas Muhammadiyah Malang, 2011.
8. Robertson, S., *Understanding inverse document frequency: on theoretical arguments for IDF*. Journal of documentation, 2004. 60(5): p. 503-520.
9. Simanullang, J.W., A. Adiwijaya, and S. Al Faraby, *Klasifikasi Sentimen Pada Movie Review Dengan Metode Multinomial Naïve Bayes.* eProceedings of Engineering, 2017. 4(2).