IJCIT (Indonesian Journal on Computer and Information Technology)
Vol.2 No.1, Mei 2017, pp. 53~60
ISSN: 2527-449X
E-ISSN**:** 2549-7421

Aplikasi *Filtering of Spam Email* Menggunakan *Naïve Bayes*

Ratih Yulia Hayuningtyas
STMIK Nusa Mandiri Jakarta
Ratih.winziy@gmail.com

Abstrak

Email merupakan alat yang penting digunakan untuk berkomunikasi, mentransfer *file* serta digunakan untuk media iklan melalui internet. Penggunaan *email* semakin meningkat maka banyak pihak lain yang mengirimkan *email* dengan pesan yang berisikan virus, penipuan, iklan dan pornografi. *Email* ini disebut dengan *spam email* atau *email* yang tidak diiginkan oleh penerima yang dikirim secara masal. Banyak pengguna merasa terganggu karena banyaknya waktu yang dihabiskan untuk menghapus pesan *spam*, biaya yang harus dikeluarkan dan besarnya bandwith jaringan yang digunakan. Untuk mengatasi masalah ini, perlu metode klasifikasi untuk membedakan antara spam dan non spam. Metode klasifikasi yang digunakan adalah Naïve Bayes merupakan metode penyaringan yang paling popular. Evaluasi menggunakan *confusion matrix* yang menghasilkan akurasi sebesar 75,9%.
Kata Kunci*: email, spam, naive bayes*

Abstract

Email is an important entity that used for digital communication in the internet, it is used to transfer information in the form of file and be used for media advertising. Increasing users email many parties to bombard multiple emails with unsolicited message that contain the promotion of product or service, pornography, viruses and that are not important. This email is called spam email message or email that are unwanted by the recipient an sent in bulk. Many users troubled by spam, such as the time wasted by useless to remove spam, the amount of network bandwidth that used, the costs to be incurred to remove spam and spent the space provided by the server. To solve this problem, need a method of classification to distinguish between spam and non spam. Classification method used is Naïve Bayes is a method of filtering the most popular. Evaluation by confusion matrix that generates 75,9% accuracy.
Keywords: *email, spam, naïve bayes*

1. PENDAHULUAN

Informasi dalam bentuk teks didapatkan dari berbagai sumber seperti buku, surat kabar, situs web ataupun pesan *email* (Ling dkk, 2014). *Email* merupakan suatu entitas penting yang digunakan untuk berkomunikasi digital melalui internet (Andriansyah dan Suhendra, 2005), selain itu digunakan untuk transfer informasi berupa *file* bahkan dapat digunakan untuk media iklan (Widiasari dan Bayu, 2013). Pesan Elektronik menjadi primadona untuk berkomunikasi saat ini. Hanya terhubung dengan koneksi internet, berkirim pesan elektronik dapat dengan mudah dilakukan (Andros dkk, 2015).

Semakin banyak orang yang terhubung ke internet menjadikan *email* sebagai salah satu alat komunikasi paling cepat dan ekonomis (Ananda, 2011). Peningkatan penggunaan *email* dapat dilihat dari beberapa tahun terakhir dari 36% pada tahun 2002, 45% pada tahun 2003 menjadi 64% pada tahun 2004, 80% pada tahun 2006, 92% pada tahun 2009 dan 95% pada tahun 2010 (Bajaj dan Pieprzyk, 2014).

Fasilitas yang dimiliki *email* memberikan kemudahan untuk mengirimkan email ke beberapapun jumlah penerimanya (Widiasari dan Bayu, 2013), selain itu *email* dimanfaatkan untuk berhubungan antar teman atau kolega dan sebagai salah satu media penyebaran berita dalam bidang *electronic commerce* (Ananda, 2011). Dengan Meningkatnya pengguna *email* memikat beberapa pihak untuk memborbardir *email* dengan pesan yang tidak diminta (Andros dkk, 2015) yang berisi promosi produk atau jasa, pornografi, virus dan hal-hal yang tidak penting (Widiasari dan Bayu, 2013). *Email* inilah yang disebut dengan *spam*

Diterima Desember 23, 2016; Revisi April 10, 2017; Disetujui April 21, 2017

email penerimanya (Widiasari dan Bayu, 2013). *Spam* merupakan pesan atau *email* yang tidak diinginkan oleh penerimanya dan dikirimkan secara massal (Adisantoso dan Rahman, 2013).

Mengirimkan *email spam* adalah sebuah pelanggaran terhadap *Acceptable Use Policy* (AUP) atau peraturan penggunaan yang bisa diterima pada hampir semua *Internet Service Provider* (ISP), dan dapat menyebabkan penghapusan pada *account* pengirim (Ananda, 2011).

Banyak pengguna *email* yang merasa terganggu dengan adanya *spam* (Supri, 2010). Dampak buruk yang paling utama dari *spam email* adalah waktu yang terbuang dengan percuma untuk menghapus spam (Widiasari dan Bayu, 2013). Besarnya *bandwidth* jaringan yang dikeluarkan (Supri dan Indra, 2010). Biaya yang harus ditanggung untuk menghilangkan atau menghapus *spam* (Andriansyah dan Suhendra, 2005). Dan menghabiskan *space* yang disediakan oleh *server* (Andros dkk, 2015).

Permasalahan ini menjadi permasalahan yang penting untuk dipecahkan (Andros dkk, 2015). Untuk mengatasi hal ini diperlukan suatu filter antispam dengan algoritma tertentu yang dapat memisahkan antara *spam-mail* dengan *non spam mail* (Supri, 2010). Banyak algoritma yang dapat digunakan dalam pemfilteran *email* diantaranya *Naïve Bayes, Support Vector Machine, Neural network, K-NN* dan lain-lain (Awad dan Elseoufi, 2011). Pada penelitian ini algoritma yang digunakan yaitu *Naïve Bayes* merupakan salah satu metode filtering yang paling popular (Widiasari dan Bayu, 2013).

TINJAUAN PUSTAKA

Email

Email adalah cara yang efektif untuk berkomunikasi satu dengan lainnya (Widiasari dan Bayu, 2013). *E-mail* (*Electronic Mail*) atau surat elektronik sudah mulai dipakai pada tahun 1960 (Widiasari dan Bayu, 2013). *Email* terdiri dari 3 komponen (Widiasari dan Bayu, 2013):

a) Envelope
Proses ini digunakan oleh *Mail Transport Agent* (MTA) untuk melihat rute atau jalur pesan.

b) Header
Digunakan sebagai informasi mengenai *e-mail* tersebut, mulai dari alamat pengirim, penerima, subjek dan lain-lain.

c) Body
Merupakan isi pesan dari pengirim ke penerima. Dalam *mail body* juga terdapat *file attachment* yang digunakan untuk mengirimkan *e-mail* berupa *file* (*mail attachment*).

Spam Email

SPAM merupakan akronim dari *Stupid Pointless Annoying Message* (Ananda, 2011). *Spam email* yaitu *email* yang tidak diinginkan atau diminta oleh penerimanya (Widiasari dan Bayu, 2013). *Spam* muncul pertama kali pada bulan mei tahun 1978. *Spam* tersebut bersifat iklan yang dikirimkan oleh *Digital Equipment Corporation* (DEC) (Widiasari dan Bayu, 2013). *Spam* juga dapat berupa pengiriman pesan secara berulang-ulang ke berbagai *newsgroup* atau *server* milis dengan pokok bahasan yang tidak berkaitan (Ananda, 2011).

Tipe-tipe *email spam* (Supri, 2010):

1. Iklan
2. *Spam* dapat digunakan untuk mempromosikan suatu produk ataupun layanan.
3. Mengirimkan *Malware*
4. *Spam* merupakan salah satu cara utama untuk mendistribusikan virus dan *malware.*
5. *Phising*
6. Bersembunyi dibalik nama besar perusahaan, lembaga keuangan, lembaga pemerintah, lembaga amal, para *phiser* mencoba memikat korban untuk mengunjungi *website* palsu.
7. *Scam*
8. Berita elektronik dalam internet yang bersifat menipu sehingga pengirimnya dapat mendapatkan manfaat atau keuntungan.
9. Pesan yang tak berarti
10. Sebuah potongan pesan sampah seperti ini dapat memenuhi *inbox mail* kita.

Klasifikasi

Klasifikasi adalah proses dengan model yang menggambarkan dan membedakan kelas data atau konsep. Model merupakan analisis objek yang label kelasnya belum diketahui (Widiasari dan Bayu, 2013).

Klasifikasi merupakan salah satu metode dalam data mining yang dapat mengklasifikasikan *email* sebagai *spam* atau *non spam*. Pengklasifikasian ini berdasarkan karakteristik dari spam (Supri, 2010):

1. Alamat pengirim yang tidak benar
2. Pemalsuan *header mail* untuk menyembunyikan *email* sesungguhny*.*
3. Identitas penerima tidak nyata.
4. Kamus alamat penyerang. Alamat *email* yang berada dalam '*To*' memiliki variasi alamat email penerima.
5. Isi *subject* tidak berhubungan dengan isi *email*.
6. Isi *email* memiliki sifat keragu-raguan.
7. *Unsubscribe* tidak bekerja pada *spam mail*.
8. Mengandung *script* tersembunyi

Data Mining

Data Mining merupakan proses pengekstraksian informasi dari sekumpulan data yang sangat besar melalui penggunaan algoritma dan teknik penarikan dalam bidang statistik, pembelajaran mesin dan sistem manajemen basis data (Teli dan Biradar, 2014).

Salah satu rangkain proses, data mining dapat dibagi menjadi beberapa tahap proses. Tahap-tahap tersebut bersifat interaktif, pemakai terlibat langsung atau dengan perantaraan *knowledge base.* Tahap-tahap data mining adalah sebagai berikut (Sukardi dkk, 2014):

1. Pembersihan Data (*DataCleaning*)
   Pembersihan data merupakan proses menghilang-kan *noise*.
2. Integrasi Data (*Data Integration*)
   Integrasi data merupakan penggabungan data dari berbagai *database* ke dalam satu *database* baru.
3. Seleksi Data (*Data Selection*)
   Data yang ada pada *database* sering kali tidak semuanya dipakai, oleh karena itu hanya data yang sesuai untuk dianalisis yang akan diambil dari *database*.
4. Transformasi Data (*Data Transformation*)
   Data diubah atau digabung ke dalam format yang sesuai untuk diproses dalam Data Mining
5. Proses Mining
   Merupakan suatu proses utama saat metode diterapkan untuk menemukan pengetahuan berharga dan tersembunyi dari data. Beberapa metode yang dapat digunakan berdasarkan pengelompokkan Data Mining.
6. Evaluasi Pola (*Pattern Evaluation*)
   Untuk mengidentifikasi pola-pola menarik ke dalam *knowledge based* yang ditemukan.
7. Presentasi Pengetahuan (*Knowledge Presentation*)
   Merupakan visualisasi dan penyajian pengetahuan mengenai metode yang digunakan untuk memperoleh pengetahuan yang diperoleh pengguna.

Algoritma *Naïve Bayes*

Naïve Bayes merupakan suatu metode klasifikasi yang menggunakan perhitungan probabilitas (Ling dkk, 2014). Teori *Naïve Bayes* diadopsi dari nama penemunya yaitu Thomas Bayes sekitar tahun 1950 (Andriansyah dan Suhendra, 2005). *Naïve Bayes* menghitung sekumpulan probabilitas dengan menjumlahkan frekuensi dan kombinasi nilai dari *dataset* yang diberikan (Sukardi dkk, 2014).

Keuntungan menggunakan *Naïve Bayes*, metode ini hanya membutuhkan jumlah data pelatihan (*Training Data*) yang kecil untuk menentukan estimasi parameter yang diperlukan dalam proses pengklasifikasian (Sukardi dkk, 2014)..

Persamaan Metode *Naïve Bayes* (Sukardi dkk, 2014).:

$$P(H|X) = \frac{P(X|H).P(H)}{P(X)}$$

Dimana:

X : Data dengan *class* yang belum diketahui

H : Hipotesis data merupakan suatu *class* spesifik

P(H|X) : Probabilitas hipotesis *H* berdasar kondisi *X* (*posterior* probabilitas)

P(H) :Probabilitas hipotesis *H* (*prior* probabilitas)

P(X|H) : Probabilitas *X* berdasarkan kondisi pada hipotesis *H*

P(X) : Probabilitas *X*

Proses klasifikasi memerlukan sejumlah petunjuk untuk menentukan kelas apa yang cocok bagi sampel yang dianalisis tersebut. Metode *Naïve Bayes* diatas disesuaikan sebagai berikut:

$$P(C|F1 \dots Fn) = \frac{P(C)P(F1 \dots Fn|C)}{P(F1 \dots Fn)}$$

Dimana variable *C* merepresentasikan kelas, sementara variable $F_1..F_n$ merepresentasikan karakteristik petunjuk

$$Posterior = \frac{prior\ x\ likelihood}{evidence}$$

yang dibutuhkan untuk melakukan klasifikasi. Rumus diatas menjelaskan bahwa peluang masuknya sampel karakteristik tertentu dalam kelas *C (Posterior)* adalah peluang munculnya kelas *C* (Sebelum masuknya sampel tersebut, seringkali disebut *prior*) dikali dengan peluang kemunculan karakteristik-karakteristik sampel pad akelas *C* (disebut juga *Likeihood*) dibagi dengan peluang kemunculan karakteristik-karakteristik sampel secara global (disebut juga *evidence*). Rumus dapat ditulis sebagai berikut:

Nilai *evidence* selalu tetap untuk setiap kelas pada suatu sampel. Nilai dari *posterior* tersebut nantinya akan dibandingkan dengan nilai-nilai *posterior* kelas lainnya untuk menentukan ke kelas apa suatu sampel akan diklasifikasikan.

Confusion Matrix

Confusion Matrix adalah alat visualisasi yang biasa digunakan pada *supervised learning*. Tiap kolom pada matriks adalah contoh kelas prediksi, sedangkan tiap baris mewakili kejadian dikelas yang sebenarnya (Gorunescu, 2011).

Tabel 1. *Confusion Matrix*

Predication	Actual	
	Positif	Negatif
True	TP	FN
False	FP	TN

Sumber Sukardi dkk,2014

Keterangan:
TP : *True* Positif
TN : *True* Negatif
FP : *False* Positif
FN : *False* Negatif

True Positif adalah jumlah *record* positif yang diklasifikasikan sebagai positif, *false* positif adalah jumlah *record* negatif yang diklasifikasikan sebagai positif, false negatif adalah jumlah *record* positif yang diklasifikasikan sebagai negatif, *true* negatif adalah jumlah *record* negatif yang diklasifikasikan sebagai negatif (Andriani, 2013).

Evaluasi yang akan dilakukan menggunakan parameter *F-Measure* yang terdiri dari perhitungan *precision*, dan *recall*. *Recall, precision* dan *F-measure* merupakan metode pengukuran yang efektifitas dilakukan pada proses klasifikasi (Supri, 2010).

Recall dan *precision* adalah dua kriteria yang digunakan untuk mengevaluasi tingkat efektivitas kinerja sistem temu kembali informasi (Supri, 2010).

a. *Precision*
Precision (*P)* adalah ukuran banyaknya dokumen yang ditemukan relevan (Ling dkk, 2014).
Precision (p) = $\frac{TP}{TP + FP}$

b. *Recall*
Recall (*R)* adalah ukuran banyak dokumen yang relevan dapat ditemukan kembali (Ling dkk, 2014).
Recall (r) = $\frac{TP}{TP+FN}$

c. *Accuracy*
Accuracy adalah persentase dari total *e-mail* yang benar diidentifikasi (Supri, 2010).
Accuracy = $\frac{TP+TN}{TP + FP + TN +FN}$

Evaluasi dengan *confusion matrix* menghasilkan nilai *sensitivity, specificity, ppv* dan *npv*. Pengukuran dengan *confusion matrix* menampilkan perbandingan dari hasil akurasi metode *Naïve Bayes*.

a. *Sensitivity*
Untuk membandingkan jumlah *true* positif terhadap jumlah *record* true positif dan *true* negatif
Sensitivity = $\frac{TP}{TP + TN}$

b. *Specificity*
Untuk membandingkan jumlah *true* negatif terhadap jumlah *record true* negatif dan *false* positif
Specificity = $\frac{TN}{TN + FP}$

c. *PPV*
Untuk membandingkan jumlah *true* positif terhadap jumlah *record true* positif dan *false* positif
PPV = $\frac{TP}{TP + FP}$

d. *NPV*
Untuk membandingkan jumlah *true* negatif terhadap jumlah *record true* negatif dan *false* negatif

$$NPV = \frac{TN}{TN + FN}$$

Bahasa Pemrograman

Hyper Text Markup Language (HTML) adalah sebuah bahasa *markup* yang digunakan untuk membuat sebuah halaman web dan menampilkan berbagai informasi didalam sebuah *browser* internet (Saleh, 2015).

PHP merupakan singkatan dati *Hypertext Processor* yaitu suatu bahasa pemrograman yang berbasiskan kode-kode atau *script* yang digunakan untuk mengolah suatu data dan mengirimkannya kembali ke web *browser* menjadi kode HTML (Oktavian, 2010)

MySQL merupakan *software* yang tergolong *database* server dan bersifat *open source*. *Open source* menyatakan bahwa *software* ini dilengkapi dengan *source code*, selain itu tentu saja bentuknya *executeable*-nya atau kode yang dapat dijalankan secara langsung dalam sistem operasi (Kadir, 2009).

2. METODE PENELITIAN

Metode Penelitian yang digunakan pada penelitian ini sebagai berikut:

a. Pengumpulan Data
   Pengumpulan data merupakan tahap awal yang digunakan sebagai masukan. Data yang digunakan diperoleh dari data UCI *Machine Learning Repository*. Data terdiri dari 4601, dimana 1813 (39,4%) adalah *spam* dan 2788 (60,6%) adalah *non spam*.
b. Metode yang digunakan
   Metode yang diggunakan dalam penelitian ini yaitu *Naïve Bay*es. Metode *Naïve Bayes* sangat baik digunakan untuk pengklasifikasian, selain itu metode ini digunakan untuk memprediksi suatu kejadian pada masa yang akan datang, dengan cara membandingkan data atau *evidence* (bukti) yang ada pada masa lampau.
c. Pengujian Metode
   Untuk pengujian metode dilakukan dengan data *spam email* yang diperoleh dari data UCI *Machine Learning Repository* yang telah diklasifikasikan kedalam *class spam* atau *non spam*. Dari data ini akan dihitung nilai probabilitas *prior* dari setiap *class*, kemudian dihitung nilai probabilitas *prior* dari setiap atribut yang ada. Setelah mendapat nilai probabilitas *prior* atribut didapatkan nilai probabilitas *posterior* untuk menentukan *class* pada data baru.
d. Evaluasi dan Validasi Hasil
   Evaluasi dan validasi hasil dilakukan dengan menghitung nilai *accuracy, precision* dan *recall.* Sedangkan untuk akurasi di ukur dengan *confusion matrix* dan kurva ROC untuk mengukur nilai AUC (*Area Under Curve*).
e. *Prototype*
   Pada penelitian ini dibuatkan GUI (*Graphical User Interface*) yaitu suatu antarmuka pada sistem yang menggunakan menu grafis agar mempermudah penggunanya untuk berinteraksi dengan komputer. Aplikasi ini dibuat untuk menguji data yang belum diketahui *class*nya.

3. HASIL DAN PEMBAHASAN

3.1. Data

Data *spam email* terdapat 58 atribut dan 1 atribut target atau *class,* sebagai berikut:

a. 48 atribut bertipe *continuous* [0,100] yang beranggotakan kata terdiri dari:
   Make, Address, All, 3d, Our, Over, Remove, Internet, Order, Mail, Receive, Will, People, Report, Addresses, Free, Business, Email, You, Credit, Your, Font, 000, Money, HP, Hpl, George, 650, Lab, Labs, telnet, 857, Data, 415, 85, Technology, 1999, Parts, Pm, Direct, Cs, Meeting, original, Project, Re, Edu, Table, Conference.
   Nilai presentase diperoleh dari:
   $$\frac{\text{Jumlah kata yang muncul dalam e-mail}}{\text{Total keseluruhan kata dalam e-mail}} \times 100\%$$
b. 6 atribut bertipe continuous [0,100] yang beranggotakan karakter terdiri dari:
   ; (| ! $ #
   Nilai presentase diperoleh dari:
   $$\frac{\text{Jumlah karakter yangmuncul dalam e-mail}}{\text{Total keseluruhan karakter dalam e-mail}} \times 100\%$$
c. 1 atribut bertipe *continuous real* [1…] yang berisi rata-rata huruf *capital.*
d. 1 atribut bertipe *continuous real* [1…] yang berisi nilai terpanjang huruf *capital.*
e. 1 atribut bertipe *continuous real* [1…] yang berisi jumlah huruf *capital.*

3.2. Menghitung Probabilitas *Prior*

Menghitung nilai probabilitas *prior* berdasarkan data yang lalu. Total keseluruhan data 4601 dengan total data *spam* 1813 dan data *non spam* 2788 dengan perhitungan sebagai berikut:

P (Spam) = 1813/4601 = 0,394
P (Non Spam) = 2788/4601 = 0,606

Nilai probabilitas *prior* dari setiap *class* didapatkan yaitu untuk nilai *spam* nilai probabilitas *prior* sebesar 0,394 dan untuk non *spam* nilai probabilitas *prior* sebesar 0,606. Setelah menghitung nilai probabilitas *prior* secara keseluruhan, kemudian menghitung nilai probabilitas *prior* dari setiap atribut dengan menggunakan metode *Naïve Bayes*.

Contoh perhitungan probabilitas *prior* untuk atribut, atribut yang digunakan sebagai contoh sebanyak 6 atribut:

Tabel 2. Probabilitas Prior Atribut

Atribut		Jumlah Data	Spam	Non Spam	P(X|C)	
					Spam	Non Spam
Kata	Address (Ya)	898	625	273	0,169	0,074
	Address (Tidak	3703	1188	2515	1,323	2,801
	Internet (Ya)	824	619	205	0,751	0,249
	Internet (Tidak)	3777	1194	2583	0,316	0,684
	Mail (Ya)	1302	827	475	0,635	0,365
	Mail (Tidak)	3299	986	2313	0,299	0,701
	Email (Ya)	1038	688	350	0,663	0,337
	Email (Tidak)	3563	1125	2438	0,316	0,684
	Money (Ya)	735	681	54	0,927	0,073
	Money (Tidak)	3866	1132	2734	0,293	0,707
	Project (Ya)	327	47	280	0,144	0,856
	Project (Tidak)	4274	1765	2508	0,413	0,587

3.3. Menghitung Probabilitas *Posterior*

Nilai probabilitas *posterior* digunakan untuk menentukan *class* terhadap data baru, berikut contoh dari probabilitas *posterior*.

Tabel 3. Probabilitas *Posterior*

Data X		P (X|C)	
Atribut	**Nilai**	**Spam**	**Non Spam**
Address	Tidak	1,323	2,801
Internet	Ya	0,751	0,249
Mail	Tidak	0,299	0,701
Email	Tidak	0,316	0,684
Money	Ya	0,927	0,073
Project	Ya	0,144	0,856

Dari tabel 2 dapat diketahui terdapat suatu data yang memiliki atribut *internet, money* dan *project* tetapi tidak ada atribut *address, mail, dan email*. Dari data tersebut dapat diketahui nilai *spam* dan *non spam* yang diperoleh dari nilai probabilitas *prior*. Kemudian menghitung total keseluruhan nilai probabilitas *posterior* dari setiap *class*, sebagai berikut:

P(X|Spam)
= P(Address|Spam) * P(Internet|Spam) * P(Mail|Spam) * P(Email|Spam) * P(Money|Spam) * P(Project|Spam)
= 1,323 * 0,751 * 0,299 * 0,316 * 0,927 * 0,144
= **0,0125**
P(X|Non Spam)
= P(Address|Non Spam) * P(Internet|Non Spam) * P(Mail|Non Spam) * P(Email|Non Spam) * P(Money|Non Spam) * P(Project|Non Spam)
= 2,801 * 0,249 * 0,701 * 0,684 * 0,073 * 0,856
= **0,0209**
P(X|Spam) * P(Spam)
= 0,0125 * 0,394
= **0,004925**
P(X|Non Spam) * P(Non Spam)
= 0,0209 * 0,606
= **0,0126654**

Dari hasil diatas dapat disimpulkan bahwa P(X|Spam) lebih kecil nilai probabilitas *posterior* dibandingkan dengan nilai P(X|Non Spam), maka dapat diketahui bahwa data diatas termasuk kedalam *class Non Spam*.

3.4. Evaluasi dan Validasi

Evaluasi dan validasi dari penelitian ini digambarkan pada tabel hasil confusion matrix dengan *Naïve Bayes* pada tabel 4.

Tabel 4. Hasil *Confusion Matrix*

	True Spam	True Non Spam
Pred. Spam	1059 (TP)	353 (FN)
Pred. Non Spam	754 (FP)	2435 (TN)

Berdasarkan dari tabel diatas dari 2788 data non spam, ternyata 353 data diprediksi spam hasilnya spam, sedangkan 2435 sesuai dengan prediksi yaitu non spam. Sebaliknya untuk data spam sebanayak 1813, data sebanyak 1059 sesuai dengan prediksi yaitu spam, sedangkan untuk 754 yang di prediksi data spam ternyata tidak sesuai. Menghitung nilai *precision, recall* dan *accuracy.*

1. *Precision* = $\frac{1059}{1059 + 754}$ = 0,584

2. *Recall* = $\frac{1059}{1059 + 353}$ = 0,75

3. *Accuracy* = $\frac{1059 + 2435}{1059 + 754 + 2435 + 353}$ = **0,759**

Nilai *accuracy* yang didapat sebesar 0,759, nilai *precision* 0,584 dan nilai *recall* sebesar 0,75. Menghitung nilai *sensitivity, specificity, ppv* dan *npv.*

1. *Sensitivity* = $\frac{1059}{1059 + 2435}$ = 0,303

2. *Specificity* = $\frac{1059}{2435 + 754}$ = 0,332

3. *PPV* = $\frac{1059}{1059 + 754}$ = 0,584

4. *NPV* = $\frac{2435}{2435 + 353}$ = 0,873

Nilai *sensitivity* yang didapat sebesar 0,303, nilai *specificity* sebesar 0,332, nilai *PPV* sebesar 0,584 dan nilai *NPV* sebesar 0,873.

3.5. Aplikasi Pemfilteran Spam *Email*

Tampilan aplikasi pada penelitian ini meliputi tampilan menu utama, menu *login e-mail,* menu *inbox,* menu spam, menu *login* aplikasi spam.

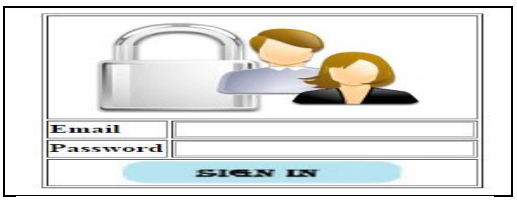
a. Tampilan Menu Utama

Tampilan Menu Utama pada penelitian ini dapat dilihat pada gambar 1.

Gambar 1. Tampilan Menu Utama

b. Tampilan Menu *Login E-mail*

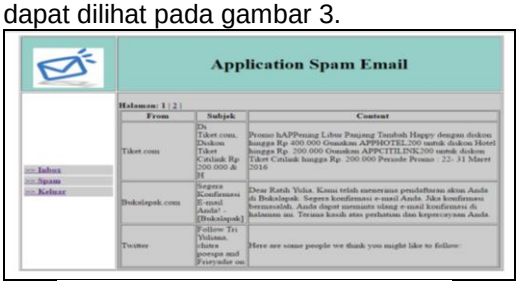
Tampilan Menu *Login E-mail* pada penelitian ini dapat dilihat pada gambar 2.



Gambar 2. Tampilan Menu *Login E-mail*

c. Tampilan Menu *Inbox*

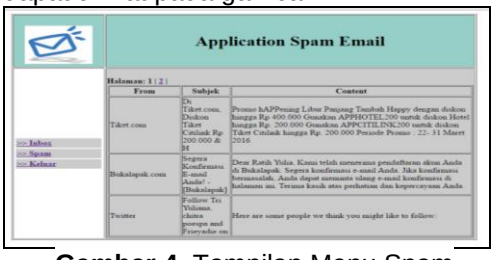
Tampilan Menu *Inbox* pada penelitian ini dapat dilihat pada gambar 3.



Gambar 3. Tampilan Menu *Inbox*

d. Tampilan Menu Spam

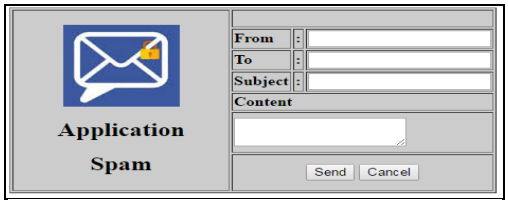
Tampilan Menu Spam pada penelitian ini dapat dilihat pada gambar 4.



Gambar 4. Tampilan Menu Spam

e. Tampilan Menu *Login* Aplikasi Spam

Tampilan Menu *Login* Aplikasi Spam pada penelitian ini dapat dilihat pada gambar 5.



Gambar 5. Tampilan Menu *Login* Aplikasi Spam

Dari hasil penelitian menggunakan *confusion matrix* bahwa pengujian yang dilakukan *Naïve Bayes* sudah baik karena memiliki akurasi 75,9%. Aplikasi dapat mengklasifikasikan suatu pesan email digolongkan sebagai spam atau bukan spam serta pengguna tidak merasa terganggu lagi karena spam yang masuk tidak tercampur dengan inbox email.

4. KESIMPULAN

Dari penelitian ini dapat ditarik kesimpulan yaitu tidak perlu menghabiskan waktu yang banyak untuk menghapus spam yang masuk ke dalam email, metode Naïve Bayes sangat baik untuk mendukung keputusan dalam pengklasifikasian. Untuk meningkatkan hasil akurasi dapat ditambahkan *feature selection* seperti *Information Gain*, *Genetic Algoritma*, untuk penelitian berikutnya bisa menggunakan metode pengklasifikasin yang lain seperti *Support Vector Machine* atau *Algoritma C.45* dan sebagainya.

REFERENSI

Adisantoso, Julio, dan Rahman, Wildan. Pengukuran Kinerja Spam Filter Menggunakan Graham's Naïve Bayes Classifier. ISSN: 2089-6026. Jurnal Ilmu Komputer Agri-Informatika Vol. 2 No. 1. 2013.

Ananda, Dahliar. Pembangunan Aplikasi Pemfilteran Email Spam Dengan Menggunakan Metode Pembeda Markov. Jurnal Teknologi Informasi Politeknik Telkom Vol.1 No.1 Mei 2011.

Andriani, Anik. Sistem Pendukung Keputusan Berbasis Decision Tree Dalam Pemberian Beasiswa Studi Kasus: AMIK "BSI Yogyakarta". ISSN: 2089-9815. Seminar Nasional Teknologi Informasi dan Komunikasi 2013, 09 Maret 2013.

Andriansyah, Miftah, dan Suhendra, Adang. Metode Penyaringan Email yang tidak Diinginkan Menggunakan Pendekatan Probabilistik. ISBN: 979-756-061-6. Seminar Nasional Aplikasi Teknologi Informasi 2005. Yogyakarta 18 Juni 2005.

Andros, Prawita, Dimas, Karsten, Juan, dan Vinandar, Maldy. Perbandingan Algoritma Pendektesian Spam. ISSN: 2477-0040. E-ISSN: 2460-7900. Jurnal Teknologi Terpadu Vol. 1 No.1 Juli 2015.

Awad, W.A, dan Elseuofi, S. M. Machine Learning Methods for Spam E-Mail Classification. International Journal of Computer Science & Information Technology (IJCSIT) Vol. 3 No. 1, Februari 2011.

Bajaj, K, dan Pieprzyk, J. A Case Study of User-Level Spam Filtering. 2014.

Gorunescu F. Data Mining Concept Model Technique. 2011.

Kadir, A. Membuat Aplikasi Web dengan PHP dan Database MySQL. Andi Offset: Yogayakarta. 2009.

Ling, Juen, Kencana, I Putu Eka N, dan Oka, Tjokorda Bagus, Analisis Sentimen Menggunakan Metode Naïve Bayes Classifier Dengan Seleksi Fitur Chi Square. ISSN: 2303-1751. E-Jurnal Matematika Vol.3 (3), Agustus 2014, pp. 92-99.

Oktavian, Diar Puji. Menjadi Programmer Jempolan menggunakan PHP. Yogyakarta: Mediakom. 2010.

Saleh, Alfa. Implementasi Metode Klasifikasi Naïve Bayes Dalam Memprediksi Besarnya Penggunaan Listrik Rumah Tangga. ISSN: 2354-5771. Citec Journal, Vol. 2 No. 3. Mei 2015-Juli 2015.

Sukardi, Syukur, Abd, dan Supriyanto, Catur. Klasifikasi Spam Email Menggunakan Algoritma C4.5 dengan Seleksi Fitur. ISSN: 1414-9999 Jurnal Teknologi Informasi, Vol. 10 No. 1, April 2014.

Supri Prayitno, Indra. Kupas tuntas Malware. Jakarta: PT. Elex Media Komputindo. 2010.

Teli, Savita Pundalik, dan Biradar, Santoshkumar. Effective Email Classification for Spam and Non-Spam. ISSN: 2277 128X. International Journal of Advanced Research in Computer Science and Software Engineering Vol. 4 Issue 6, June 2014.

Widiasari, R Indrastanti, dan Bayu, Teguh Indra. Pembangunan Spam E-mail Filtering System dengan Metode Naïve Bayesian. Konferensi Nasional Sistem Informasi 2013.