Prosiding Seminar Nasional Teknologi Informasi Komputer dan Sains 2019
Aula AMIK Imelda, 3 Agustus 2019, AMIK IMELDA, Medan – Indonesia
http://sintaks.kitamenulis.id/index.php/Sintaks e-ISBN : 978-623-92311-0-1

Implementasi Metode Naïve Bayes Classifier dalam Melakukan Filterisasi Spam

Hery Sunandar[1], Edward Robinson Siagian[2]
STMIK Budidarma Medan, Jalan Sisingamangaraja No. 338 Simpang Limun Medan
Email : herysun1975@gmail.com[1], edwardrobin129@gmail.com[2]

ABSTRAK

Internet telah menjadi salah satu hal yang terpenting dalam perkembangan sarana komunikasi. Salah satu fasilitas yang terdapat pada internet adalah surat elektronik atau lebih dikenal sebagai e-mail. Fasilitas e-mail yang mudah digunakan dan murah mengakibatkan banyaknya e-mail yang berisi iklan dan promosi bisnis masuk kedalam inbox pengguna fasilitas *e-mail*. *E-mail* iklan inilah yang disebut sebagai spam mail. Untuk mencegah hal ini, dibuatlah software yang berguna sebagai *spam filter* untuk menyaring e-mail yang masuk kedalam inbox pengguna fasilitas e-mail. Metode naïve bayes adalah sebuah metode yang digunakan untuk melakukan filter pada email, metode ini memiliki keakuratan yang lebih tinggi. Klasifikasi email dapat dibedakan yaitu sistem klasifikasi yang beroperasi pada mail client (offline) serta mail server (online).

Kata Kunci : Email, Bayes, Artificial Intelegent.

ABSTRACT

The internet has become one of the most important things in the development of communication facilities. One of the facilities found on the internet is electronic mail or better known as e-mail. E-mail facilities that are easy to use and inexpensive result in many e-mails containing advertising and business promotions entering the inbox of e-mail users. This e-mail advertisement is referred to as spam mail. To prevent this, software that is useful as a spam filter is made to filter e-mail that comes into the user's e-mail facility inbox. Naïve Bayes method is a method used to filter e-mails, this method has a higher accuracy. Email classification can be distinguished, namely the classification system that operates on the mail client (offline) and the mail server (online).

Keywords: Email, Bayes, Artificial Intelegent.

1. Pendahuluan

Teknologi internet seperti yang kita ketahui berperan sebagai wadah dari berbagai teknologi lain didalamnya, dimana salah satunya adalah fasilitas pengirimaa surat elektronik atau yang lebih kita kenal sebagai *e-mail*. Teknologi *e-mail* seiring dengan evolusi teknologi internet telah berkembang dengan pesat, dari hanya memiliki kemampuan untuk mengirim teks kepada pengguna lain dalam sebuah jaringan tertutup, hingga memungkinkan penggunanya mengirimkan data selain teks kepada pengguna lain nya di seluruh dunia. Selain mempersingkat waktu dan memperpendek jarak, *e-mail* juga menjadi sebuah media yang sangat efektif dan efisien dalam berkomunuikasi. Tentunya hal ini juga diimbangi dengan permasalahan yang tidak kalah seriusnya. Karena dinilai sangat efektif dan efisien, acapkali teknologi *e-mail* disalah gunakan oleh pihak – pihak tertentu demi kepentingan pribadi. Bentuk – bentuk penyalah gunaan teknologi *e-mail* sangat bervariasi mulai dari sejenisnya dan tingkat ancamannya, antara lain *phising*, *spamming* dan *e-mail worms*.

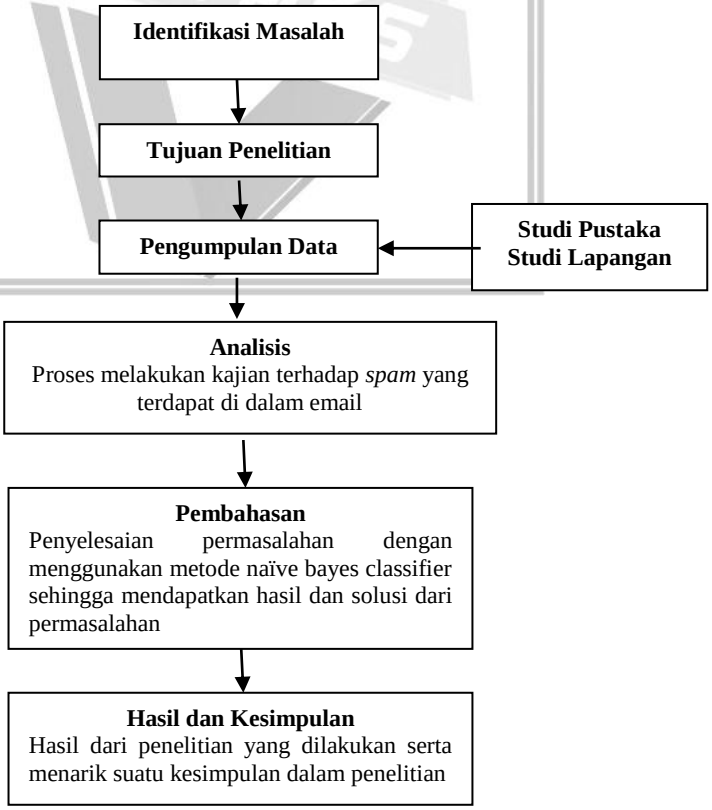
Pada penelitian terdahulu yang dilakukan oleh Miftah Andriansyah, SNATI (2005) tanggal 18 juli 2005, yogyakarta, ISBN : 979756-061-6, mengatakan bahwa proses

penyaringan berdasarkan cara kerjanya yaitu : statik dan dinamik (aktif). Metode statik adalah metode yang menggunakan software sebagai media penyaringan, sedangkan metode dinamik adalah metode yang menghitung probabilitas email terbaru yang masuk terhadap email yang telah masuk sebelumnya yang disimpan di database. Secara umum filter bayesin mengenail pesan (spam) berdasarkan pada karakteristik berupa kata-kata pada badan suatu pesan, *header*, kode HTML maupun *meta information*

Gambar 1. Database Bayes

2. Metode Penelitian

Metodologi yang digunakan pada penelitian ini menjelaskan bahwa perhitungan probabilitas suatu kejadian sekarang yang mempunyai kaitan dengan kejadian yang akan datang. Pengambilan keputusan tergantung kepada kejadian-kejadian sebelumnya. Tingkat toleransi dari suatu email sebagai spam ditentukan oleh desainernya, semakin tinggi tingkat toleransi yang dapat mengkategorikan sebagai *spam*, maka semakin tinggi pula keakurasiannya dalam melakukan pemblokiran email tersebut. Tahapan yang dilakukan peneliti dalam melaksanakan penelitian dapat dilihat pada gambar diagram alir di bawah ini.



Gambar 2. Diagram Alir

3. Hasil dan Pembahasan

Sebuah *e-mail* diterima oleh spam filter berisi pesan sebagai berikut "Hitung spam atau bukan". Berikut adalah total ditemukannya masing – masing kata pada database spam : kata 'hitung' 10 kali ditemukan, kata 'spam' 5 kali ditemukan, kata 'atau' 5 kali ditemukan, dan kata 'bukan' 15 ditemukan. Dan selanjutnya adalah total ditemukannya masing – masing kata pada database ham : kata 'hitung' 15 kali ditemukan,kata 'spam' 15 kali ditemukan, kata 'atau' 20 kali ditemukan,dan kata 'bukan' 25 kali ditemukan.

Jika total pesan yang telah diterima spam filter adalah 100 pesan, total spam yang diterima spam filter adalah 70 pesan, dan total ham (pesan tak berbahaya) adalah 30 pesan. Kategorikan pesan diatas sebagai spam / tidak menggunakan algoritma yang telah di jelaskan. Proses yang pertama dapat mengidentifikasi tiap *variable* yang akan digunakan terlebih dahulu.

P(Spam)=70/100	P(-Spam)=30/100
P(w_1|Spam)=10/70	P(w_1|-Spam)=15/30
P(w_2|Spam)=5/70	P(w_2|-Spam)=15/30
P(w_3|Spam)=5/70	P(w_3|-Spam)=20/30
P(w_4|Spam)=5/70	P(w_4|-Spam)=25/30

Setelah mengidentifikasi tiap variable, subtitusikan tiap variable kedalam

$$ln\frac{P(Spam|D)}{P(-Spam|D)} = ln\frac{P(Spam)}{P(-Spam)} + \sum_i ln\frac{P(w_i|Spam)}{P(w_i|Spam)}$$

Hingga didapat hasil sebagai berikut :

$\sum_i P(w_i|Spam)$ =ln 0,14285 + ln 0,07142 + ln 0,07142 + ln 0,21428= -8,76447

$\sum_I P(w_i|-Spam)$ =ln 0,5 + 0,5 + ln 0,66666 + in 0,83333 = -1,97408

Ln P(Spam/D) / P(-Spam/D)

= ln (0,7 / 0,3)+(-8,76447-(-1,97408)) = ln 2,33333 + (-6,79039) = 0,84729 – 6,79039 = -5,9431

Setelah didapat hasil akhir, nilai tersebut dicocokan dengan sifat berikut untuk melakukan proses pengklasifikasi

$$ln\frac{P(Spam|D)}{P(-Spam,|D)} > 0$$

Karena -5,9431<0 maka dokumen tersebut diklasifikasikan sebagai bukan spam.

4. Kesimpulan

Berdasarkan proses yang dilakukan metode *naïve bayes classifier* maka dapat disimpulkan bahwa :

1. Penyaringan email yang dilakukan oleh metode *naïve bayes classifier* sangat efektif
2. Klasifikasi spam email dengan menggunakan metode *naïve bayes classifier* dalam pengklasifikasian *email* spam secara tepat dengan tingkat *error* yang kecil

5. Daftar Pustaka

Budiharto, widodo, 2015, Artificial Intelligence (Konsep dan Penerapannya), Andi, Yogyakarta.

Miftah Andriansyah, 2005, Metode Penyaringan Email Yang Tidak Diinginkan Menggunakan Pendekatan Probabilistik, Seminar Nasional Aplikasi Teknologi Informasi (SNATI), ISBN : 979756-061-6

Jogiyanto. H.M, 2001, Pengenalan Ilmu Komputer, Andi, Yogyakarta.

Kusumadewi, Sri, 2010, Artificial Intelligence (Teknik dan Aplikasinya), Penerbit Graha Ilmu, Jakarta

Soetejo. J, 2012, Jurus Kilat Mahir Komputer, Penerbit Dunia Komputer, Jakarta

http://endraithuujelek.wordpress.com/2009/11/29/definisi-spam-atau-junk-mail/