Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Deteksi Spam Email Menggunakan Bayesian Network

Dendy Andrian[1]
Teknik Informatika Fakultas Ilmu Komputer
Universitas Sriwijaya
Palembang, Indonesia
Email : dendy.andrian@hotmail.com

Muhammad Fachrurrozi[2], Novi Yusliani[3]
Teknik Informatika Fakultas Ilmu Komputer
Universitas Sriwijaya
Palembang, Indonesia
Email : {mfachrz, novi_yusliani}@unsri.ac.id

Abstrak—***Email* telah menjadi salah satu alat komunikasi internet yang mudah dan cepat. Tetapi masih banyak masalah yang dihadapi oleh pengguna *email*. Masalah utama yang sering dihadapi adalah meningkatnya jumlah *email* yang tidak diharapkan atau yang biasa disebut *spam*. *Email spam* dapat berdampak pada penyalahgunaan koneksi internet dan sangat *Bayesian Network*, tujuannya untuk mendapatkan metode yang sesuai. Berdasarkan hasil percobaan *software* ini, akurasi hasil yang didapatkan adalah 93.33% dimana dari 30 data *email* yang diuji terdapat 2 data *email* yang tidak *valid*. *Email spam* terdeteksi karena terdapat banyak kata – kata yang mengandung iklan, pornografi dan judi dalam *email* tersebut.**

Keywords: Bayesian network*, Deteksi *spam email

I. PENDAHULUAN

Email telah menjadi salah satu alat komunikasi internet yang mudah dan cepat. Tetapi masih banyak masalah yang dihadapi oleh pengguna *email*. Masalah utama yang sering dihadapi adalah meningkatnya jumlah *email* yang tidak diharapkan atau yang biasa disebut *spam*. Pesan *spam* dapat berdampak pada penyalahgunaan koneksi internet dan sangat mengganggu pengguna. Pada umumnya, *spam* berisikan iklan, *link* situs yang tidak baik seperti pornografi dan virus yang dapat merusak komputer. Permasalahan tersebut, dapat diatasi dengan membuat sebuah anti *spam*. Anti *spam* ini berfungsi untuk mendeteksi *email* dan memberikan informasi kepada pengguna apabila terdapat suatu pesan yang memiliki potensial sebagai *spam*. Salah satu teknik untuk membuat anti *spam* adalah Bayesian *Network* (BN), yang dapat digunakan untuk memperkirakan kemungkinan bahwa pesan yang masuk adalah *spam*.

Metode Bayesian *Network* (BN) merupakan salah satu *Probabilistic Graphical Model* (PGM) yang dibangun dari teori probabilistik dan teori graf. Selain digunakan untuk mendeteksi sebuah pesan *spam*, metode BN juga dapat digunakan untuk mendiagnosa suatu penyakit [1]. Penelitian ini menggunakan algoritma Bayesian *Network* (BN) untuk mendiagnosa suatu penyakit berdasarkan gejala.[2] melakukan analisis dalam teknik *email spam*. Penelitian ini menyajikan berbagai teknik anti *spam* seperti *whitelist/blacklist*, *Support Vector Machine* (SVM) dan Bayesian *Classifier*.[3] melakukan peningkatan algoritma Bayesian untuk mendeteksi *spam email*. Penelitian ini menyatakan algoritma Bayesian memiliki akurasi yang tinggi dalam melakukan deteksi *spam* dengan menghasilkan akurasi 90%. [4] melakukan deteksi *spam email* dalam bahasa Vietnam berdasarkan klasifikasi bahasa menggunakan algoritma Bayesian. Penelitian ini menyatakan algoritma Bayesian sangat efektif diterapkan untuk bahasa Inggris dan bahasa lainnya tetapi tidak efektif pada bahasa Vietnam. Sehingga algoritma Bayesian di kombinasi berdasarkan klasifikasi bahasa dan menghasilkan akurasi 9% lebih akurat dibandingkan dengan teknik lainnya. [7] melakukan deteksi spam email menggunakan Natural language Processing (NLP). Penelitian ini menyajikan analisis terhadap teknik anti spam pada bidang ilmu NLP yang dapat digunakan dalam mendeteksi spam, salah satunya adalah Bayesian klasifikasi. [5] melakukan klasifikasi menggunakan Bayesian Network (BN). Penelitian ini menyatakan BN lebih efektif dari teknik Naive Bayes dan Tree Augmented Naive Bayes (TAN) karena memiliki ketepatan klasifikasi yang konsisten dengan menghasilkan akurasi 90,49%.

Oleh karena itu, penelitian yang dilakukan dalam tugas akhir ini yaitu mengembangkan perangkat lunak untuk mendeteksi *spam email* dengan menggunakan metode Bayesian *Network* (BN). Dengan metode ini diharapkan, metode BN dapat menjadi metode yang efektif dalam mendeteksi *spam email*.

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

II. METODE PENELITIAN

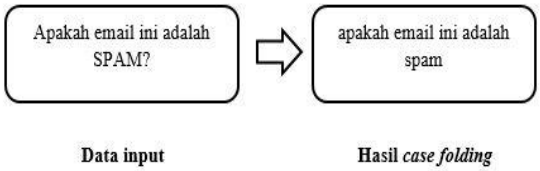
2.1. Natural Language Processing

Menurut [9] *Natural Language Processing* adalah suatu penelitian yang mengeksplorasi bagaimana komputer dapat digunakan untuk memahami dan memanipulasi teks bahasa alami untuk melakukan sesuatu yang bermanfaat.

2.2. *Preprocessing*

2.2.1. Case folding

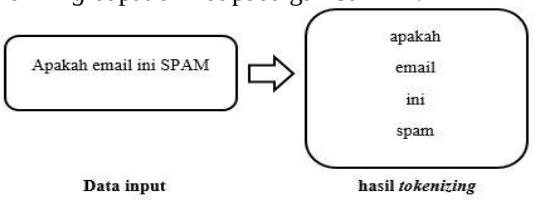
Case folding merupakan proses mengubah semua huruf dalam suatu kalimat menjadi huruf kecil. Gambar dari proses *case folding* dapat dilihat pada gambar II-1 dibawah ini :



Gambar II-1. Proses *Case Folding*

2.2.2. Tokenizing

Tokenizing adalah proses pemecahan kalimat menjadi kata-kata tunggal dilakukan dengan men-*scan* kalimat menggunakan pemisah *white space* seperti spasi, tab, dan *newline* [9]. Gambar dari proses *tokenizing* dapat dilihat pada gambar II-2.



Gambar II-2. Proses *Tokenizing*

2.3. *Bayesian Network*

BN adalah sebuah *Directed Acrylic Graph* (DAG) dan dilengkapi dengan *Conditional Probability distribution Table* (CPT) untuk setiap *nodenya.* Setiap *node* merepresentasikan sebuah *domain variable* dan setiap panah antar *node* merepresentasikan sebuah probabilistik. Secara umum BN dapat digunakan untuk menghitung probabilitas dari suatu *node* dengan memberi nilai pada *node* lain yang berhubungan.

Perhitungan nilai peluang pada struktur BN adalah dengan rumus sebagai berikut:

$$P(X_1, \ldots, X_n) = \prod P(X_i \mid \text{parents}\ (X_i))$$

Tahapan yang dilakukan untuk membangun *Bayesian Network* yang mampu mengklasifikasi *email* berdasarkan klasifikasi yang dibuat untuk mendeteksi *spam email*. Pertama – tama *email* masukan diproses dan masuk ke dalam proses pra-pengolahan yaitu *casefolding* dan *tokenizing.* Proses *casefolding* yaitu proses mengubah semua huruf dalam suatu dokumen/kalimat menjadi huruf kecil. Selanjutnya masuk ke proses *tokenizing* yaitu proses pemecahan kalimat menjadi kata-kata tunggal dilakukan dengan men-*scan* kalimat menggunakan pemisah *white space* seperti spasi, tab, dan *newline*. Setelah proses *casefolding* dan *tokenizing* dilakukan selanjutnya masuk ke proses perhitungan nilai probabilitas menggunakan metode bayesian *network*. Proses yang terakhir yaitu membandingkan nilai probabilitas *email* tersebut termasuk ke dalam kategori *spam* atau bukan *spam.*

III. HASIL PENGUJIAN

Jumlah data yang digunakan pada penelitian ini adalah sebanyak 30 *email* dengan 15 *email spam* dan 15 *email* bukan *spam.* Hasil pengujian dideskripsikan pada tabel 1.

Tabel 1. Hasil Pengujian Data *Spam*

Email	Deteksi *Email*	Deteksi Perangkat lunak	Keterangan	Nilai Peluang
Email 1	Spam	Spam	Valid	14.26
Email 2	Spam	Spam	Valid	22.12
Email 3	Spam	Spam	Valid	40.00
Email 4	Spam	Spam	Valid	45.58
Email 5	Spam	Spam	Valid	41.09
Email 6	Spam	Spam	Valid	11.21
Email 7	Spam	Spam	Valid	11.41
Email 8	Spam	Non Spam	Tidak Valid	-4.10
Email 9	Spam	Spam	Valid	11.12
Email 10	Spam	Spam	Valid	10.92
Email 11	Spam	Spam	Valid	11.49
Email 12	Spam	Spam	Valid	11.41
Email 13	Spam	Spam	Valid	15.09
Email 14	Spam	Non Spam	Valid	-8.57
Email 15	Spam	Spam	Valid	11.24

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Tabel 2. Hasil Pengujian Data Bukan *Spam*

Email	Deteksi *Email*	Deteksi Perangkat lunak	Keterangan	Nilai Peluang
Email 1	Non Spam	Non Spam	Valid	-15.5
Email 2	Non Spam	Non Spam	Valid	-6.50
Email 3	Non Spam	Non Spam	Valid	-6.17
Email 4	Non Spam	Non Spam	Valid	-7.15
Email 5	Non Spam	Non Spam	Valid	-6.26
Email 6	Non Spam	Non Spam	Valid	-34.7
Email 7	Non Spam	Non Spam	Valid	-13.1
Email 8	Non Spam	Non Spam	Valid	-19.5
Email 9	Non Spam	Non Spam	Valid	-7.64
Email 10	Non Spam	Non Spam	Valid	-2.67
Email 11	Non Spam	Non Spam	Valid	-13.3
Email 12	Non Spam	Non Spam	Valid	-6.65
Email 13	Non Spam	Non Spam	Valid	-9.28
Email 14	Non Spam	Non Spam	Valid	-9.05
Email 15	Non Spam	Non Spam	Valid	-8.25

Berdasarkan hasil pengujian dengan 30 *email*, didapatkan beberapa hasil data pengujian yang tidak valid. Pada pengujian diatas dapat dilihat bahwa terdapat 2 *email* yang tidak valid, yaitu *email* 8 dan *email* 14. Pada *email* 8 dan *email* 14 tidak terklasifikasi dengan benar karena isi dari *email* 8 dan *email* 14 lebih banyak mengandung kata bukan *spam* pada data pelatihan. Dari pengujian diatas didapatkan kesimpulan bahwa banyaknya variasi *email* pada data pelatihan sangat mempengaruhi proses klasifikasi sehingga menghasilkan data yang tidak terklasifikasi dengan benar. Dari pengujian diatas dapat dihitung akurasi pada tabel 3.

Tabel 3. Tabel Tingkat Akurasi

Klasifikasi	Valid	Tidak Valid
Spam	13	2
Bukan *Spam*	15	0
Tingkat Akurasi : $\frac{28}{30} \times 100\% = 93,33\%$		

IV. KESIMPULAN

Banyaknya variasi isi dari *email* pada data pelatihan sangat mempengaruhi proses klasifikasi sehingga menghasilkan data yang tidak terklasifikasi dengan benar. Untuk itu jumlah data harus diperbanyak semakin banyak data pelatihan semakin akurat proses klasifikasi. Dari 30 *email* yang telah diujikan dengan menggunakan 100 data pelatihan *email spam* dan 100 data pelatihan *email* bukan *spam*, persentase hasil klasifikasi *email* menjadi *spam* atau bukan *spam* menggunakan metode Bayesian *network* pada perangkat lunak sebesar 93,33%.

REFERENSI

[1] P. Suchanek, F. Marecki and R. Bucki , "Self-learning bayesian networks in diagnosis," *Procedia Computer Science*, vol. 35, pp. 1426 - 1435, 2014.

[2] C. V. K. S. and S. G. , "A study on Email Spam Filtering Techniques," *International Journal Of Computer Applications (0975 - 8887)*, pp. Volume 12 - No. 1, 2010.

[3] H. Yin and Z. Chaoyang , "An improved Bayesian Algorithm for Filtering Spam E-mail," *Internatioanl Symposium on Intelligence Information Processing and Trusted Computing*, 2011.

[4] N. T. Anh, T. Q. Anh and N. N. Binh, "Vietnamese Spam Detection based on Language Classification," *IEEE*, 2008.

[5] S. L. Ang, H. C. Ong and H. C. Low, "Classification Using the General Bayesian Network," *SCIENCE & TECHNOLOGY*, pp. 205 - 2011, 2016.

[6] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," *Expert Sytems with Application*, pp. 4321 - 4330, 2009.

[7] R. Giyanani and M. Desai, "Spam Detection using Natural Language Processing," *IOSR Journal of Computer Engineering (IOSR-JCE)*, pp. 116-119, 2014.

[8] Y. Gong and Q. Chen, "Research of Spam Filtering Based on Bayesian Algorithm," *International Conference on Computer Application and System Modeling (ICCASM 2010)*, 2010.