Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795

Sistem Deteksi Surel SPAM Dengan DNSBL Dan Support Vector Machine Pada Penyedia Layanan *Mail Marketing*

Fahri Firdausillah*, Muhammad Hafidz, Erika Devi Udayanti, Etika Kartikadarma

Fakultas Ilmu Komputer, Program Studi Sarjana Teknik Informatika, Universitas Dian Nuswantoro, Semarang
Jl. Imam Bonjol No.207, Pendrikan Kidul, Kec. Semarang Tengah, Kota Semarang, Jawa Tengah, Indonesia
Email: [1]fahri@dsn.dinus.ac.id, [2]111201509000@mhs.dinus.ac.id, [3]erika@dsn.dinus.ac.id, [4]etika@dns.dinus.ac.id
Email Penulis Korespondensi: fahri@dsn.dinus.ac.id
Submitted: **04/07/2022**; Accepted: **31/07/2022**; Published: **31/07/2022**

Abstrak−*Mail marketing* merupakan media komunikasi bagi pengguna dan penyedia jasa Internet yang efektif. Banyak perusahaan menggunakan surel sebagai media komunikasi dengan pelanggan untuk memastikan pelanggan tidak tertinggal informasi terbaru serta memberikan penawaran personal pada pelanggan tertentu. Meski demikian, tidak semua surel yang dikirim dapat sampai ke kotak masuk surel seperti yang diharapkan. Ada beberapa faktor yang mempengaruhi hal tersebut, antara lain karena konten yang tidak sesuai kaidah penulisan dan cenderung memiliki *signature* SPAM, alamat tujuan surel yang tidak valid, domain pengguna yang terdaftar dalam *blacklist* dan lain sebagainya. Penyedia layanan mail marketing seperti MTarget dan Mailchimp harus memastikan email yang dikirim oleh pelanggannya tidak berpotensi menjadi SPAM, karena dapat berdampak seluruh layanan mail marketingnya akan masuk dalam daftar hitam dan tujuan promosi tidak tercapai. Berdasarkan hal tersebut, diperlukan sistem untuk mengecek surel yang akan dikirim secara massal oleh pelanggan tersebut, serta memastikan surel tersebut tidak terdeteksi sebagai SPAM oleh aplikasi layanan surel seperti Gmail. Penelitian ini menghasilkan sebuah sistem validator surel yang dapat mencegah pengiriman email yang berpotensi menjadi SPAM, sehingga dapat mengurangi resiko sebuah penyedia layanan mail marketing masuk dalam blacklist yang berakibat terhambatnya promosi melalui email dan turunnya omzet pemasaran. Metode pengecekan yang digunakan pada penelitian ini adalah Domain Name System-Based Blackhole List (DNSBL) untuk mengecek IP dan domain pengirim dan Support Vector Machine (SVM) untuk mengecek konten surel yang akan dikirim. Sistem yang dikembangkan telah berfungsi sebagaimana yang diharapkan dan memiliki tingkat akurasi 97,54% dalam mendeteksi surel SPAM.

Kata Kunci: Deteksi SPAM; DNSBL; SVM; Sistem Pencegah; Pembelajaran Mesin

Abstract−Mail marketing is an effective communication medium for users and internet providers. Many companies use email as a mean of communication with customers to ensure customers are not left behind with the latest information, and at once provide personalized offers to specific customers. However, not all emails that are sent reach mail inbox as expected. There are several factors as the cause including content that does not comply with the writing rules and tends to have SPAM signatures, invalid e-mail addresses, the sender domains are registered in the blacklist and so forth. Mail marketing service providers such as MTarget and Mailchimp must ensure that emails sent by their customers have no potential to become spam, because it can affect all of their mail marketing services will be blacklisted, thus promotional goals will not be achieved. In that case, a system is needed to check the e-mail that will be sent by the customer, to ensure that the e-mail will not detected as a spam by email service applications such as Gmail. This research produces an email validator system that can prevent sending emails that have the potential to become SPAM, so as to reduce the risk of a mail marketing service provider being blacklisted which results in delays in promotion via email and a decrease in marketing turnover. The proposed method used in this research is the Domain Name System-Based Blackhole List (DNSBL) to check the IP and the sending domain and the Support Vector Machine (SVM) to check the content of the email to be sent. The system developed has been functioning as expected and has an accuracy rate of 97.54% in detecting SPAM emails.

Keywords: SPAM Detection; DNSBL; SVM; Prevention System; Machine Learning

1. PENDAHULUAN

Mail marketing merupakan salah satu cara yang cukup efektif untuk memberikan informasi pada pelanggan atau calon pelanggan produk tertentu [1]. Surel juga sering menjadi media bagi perusahaan untuk tetap *keep in touch* dengan pelanggannya dengan mengirimkan penawaran yang personal untuk pelanggan tertentu [2]. Meski demikian, surel *marketing* ini juga memiliki resiko yang cukup besar yaitu surel yang dikirim terdeteksi sebagai SPAM sehingga tidak dapat masuk ke dalam inbox calon pelanggan. Surel yang terdeteksi sebagai spam terkadang akan mengalami *bounce*, yaitu laporan kembali pada pengirim bahwa surel tersebut tidak terkirim, dan terkadang surel akan tetap masuk ke alamat pengguna, namun otomatis masuk pada direktori SPAM [3]. Semakin besar persentase *bounce* untuk setiap surel dikirim, semakin besar pula dampak yang negatif yang diterima baik bagi perusahaan ataupun pelanggan. Selain menurunkan nilai pemasaran, IP address ataupun DNS address dari perusahaan atau jasa pengiriman surel marketing dapat di-*banned* oleh server mail dari surel pelanggan. Proses *whitelist*/pemurnian surel yang diblokir cenderung rumit dan memakan waktu yang lama sehingga menghambat aktivitas *marketing* perusahaan dan berakibat menurunnya omset penjualan.

Resiko masuk ke dalam daftar hitam menjadi lebih besar dan lebih kritis untuk perusahaan penyedia layanan *mail marketing* seperti Mailchimp dan MTarget. Perusahan yang menyediakan layanan pengiriman personalisasi email secara massal tersebut harus memastikan bahwa email yang dikirimkan pelanggannya masuk ke dalam inbox pengguna dengan baik, sehingga tujuan dari promosi dan pemasaran tercapai. Jika ada pelanggan yang aktif mengirimkan surel SPAM melalui layanan *mail marketing*, maka aplikasi penerima email seperti Gmail

Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795

akan memasukkan layanan tersebut ke dalam daftar hitam penyebar SPAM. Akibatnya semua pelanggan lain di perusahaan tersebut juga terkena dampak secara langsung yaitu juga akan dimasukkan ke dalam kategori SPAM. Dengan demikian, surel promosi tidak akan dibaca oleh penerima, dan penyedia layanan mail marketing tersebut juga akan ditinggalkan pelanggannya.

Menurut Alkahtani [4] taksonomi untuk penyaringan spam pada surel secara umum dapat dibagi menjadi dua yaitu *Reputation-Based Filtering* dan *Content-Based Filtering*. Penyaringan kategori pertama, yaitu *Reputation-Based Filtering* adalah penyaringan spam yang penyebabnya bukan dari konten pada surel, melainkan berdasarkan *origin* pengirim surel. Penyaring tersebut membuat penilaian terhadap reputasi dari pengirim, penerima dan perantara dalam proses pengiriman pesan. Sedangkan kategori penyaringan kedua *Content-Based Filtering* adalah penyaringan spam dengan menilai apakah konten surel mengandung kalimat, link, atau pola tertentu yang sesuai dengan *signature* email SPAM.

Salah satu contoh *reputation-based filtering* adalah penyaringan SPAM berdasarkan *Domain Name System Blacklist* (DNSBL), yang merupakan daftar alamat IP yang dicurigai mengirim SPAM dan digunakan untuk mencegah pesan surel yang tidak diinginkan mencapai penerima yang tidak curiga. List ini dikumpulkan dan diperbaharui oleh penyedia layanan DNSBL secara berkala dan dapat digunakan sebagai referensi penyedia layanan surel untuk mencegah pelanggan mendapatkan surel dari pihak yang tidak diinginkan [5]. Selain dapat digunakan sebagai pencegahan penerimaan surel SPAM, DNSBL ini juga dapat digunakan sebagai penyedia layanan surel marketing seperti Mailchimp, SendInBlue, dan MTarget untuk memeriksa apakah domain yang dimiliki pelanggannya ada yang sudah masuk pada DNSBL. Pengecekan ini bertujuan agar pelanggan lain tidak terkena dampak negatif dari salah satu pelanggan yang domainnya sudah masuk dalam daftar hitam.

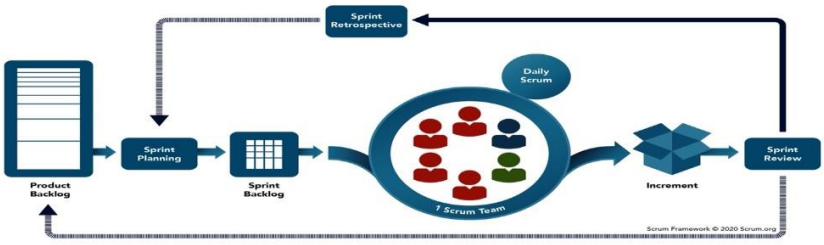
Adapun metode *content filtering* dalam deteksi SPAM dapat diimplementasikan menggunakan pembelajaran mesin dan pemrosesan bahasa natural, untuk memeriksa isi dari sebuah surel yang dikirimkan dan mengeceknya apakah memiliki ciri-ciri (*signature*) surel SPAM atau tidak [6]. Salah satu algoritma pembelajaran mesin yang dapat digunakan untuk klasifikasi dan deteksi ini adalah Support Vector Machine (SVM). SVM merupakan model pembelajaran tersupervisi yang dapat menganalisis data untuk keperluan klasifikasi ataupun regresi, namun lebih seringnya digunakan untuk klasifikasi. Arti dari pembelajaran tersupervisi adalah dataset yang digunakan harus diberikan label terlebih dahulu patokan awal [7].

Berdasarkan hal tersebut, penelitian ini bertujuan untuk mengembangkan sistem pencegah pengiriman surel SPAM agar tidak mengalami *bounce* dengan menggunakan dua metode yaitu pengecekan DNSBL untuk pengecekan *reputation-based* dan SVM untuk pengecekan dengan *content-based*. Untuk mencapai tujuan tersebut, pada penelitian ini telah dikembangkan sebuah aplikasi web untuk memastikan setiap surel yang akan dikirimkan diperiksa terlebih dahulu apakah sudah memenuhi kriteria surel yang lolos uji SPAM. Apabila memenuhi kriteria, surel yang *legitimate* akan di kirim ke alamat tujuan dan sebaliknya jika tidak maka surel tidak akan dikirim, serta pelanggan layanan *mail marketing* (pengirim surel) akan diberikan peringatan potensi SPAM. Terdapat dua manfaat utama dari deteksi dini surel SPAM ini, pertama adalah efisiensi bandwidth pada lalu lintas pengiriman surel karena berkurangnya sinyal *bounce* yang dikirimkan kembali oleh server penerima email. Kemudian manfaat kedua yang lebih penting yaitu, dengan berkuranganya sinyal *bounce* juga berarti mengurangi resiko sebuah layanan *mail marketing* masuk ke dalam daftar hitam aplikasi pengelola surel seperti Gmail [8].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian dan Pengembangan Sistem

Metode yang digunakan pada penelitian ini, sekaligus digunakan untuk proses pengembangan sistemnya mengadopsi kerangka kerja SCRUM. Metode ini menggunakan kerangka kerja yang ringan, berulang, dan bertahap untuk mengelola pengembangan produk [9]. Secara umum tahapan penelitian pada kerangka kerja SCRUM ditunjukkan pada Gambar 1, di mana penelitian dimulai dari aktivitas menyusun product backlog dibuat untuk menentukan visi besar dari penelitian berdasarkan reviu literatur. Tahapan selanjutnya adalah sprint planning untuk memecah product backlog ke dalam beberapa sprint backlog yang akan dikerjakan dalam beberapa siklus sprint. Setiap penyelesaian deliverables pada Sprint, sub produk akan dikonsultasikan kepada stakeholder untuk mendapatkan umpan balik dan pengembangan berupa product increment. Semua proses tersebut akan dilakukan secara berulang hingga keseluruhan sistem selesai dikembangkan.



Gambar 1. Alur Kerangka Kerja SCRUM

Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795

Secara kongkrit tahapan penelitian dan pengembangan sistem adalah sebagai berikut:

a. Pembuatan product backlog visi utama pengembangan sistem yaitu sistem yang dapat mencegah pengiriman surel SPAM dengan cek DNSBL dan content filtering menggunakan SVM dengan menggunakan reviu literatur.
b. Sprint planning dilakukan untuk merencanakan desain penelitian serta memecah product backlog menjadi beberapa sub komponen yang dapat dikerjakan secara terpisah, meliputi komponen Scraping DNSBL, komponen SVM model generator, komponen pengecekan surel, dan terakhir adalah komponen frontend untuk berinteraksi dengan pengguna akhir. Hasil dari tahapan ini adalah sprint backlog.
c. Pada tahapan daily scrum dilakukan pengembangan komponen sistem yang sudah tercantum pada dokumen sprint backlog. Selain aktivitas pengembangan, pada tahapan ini juga dilakukan pengumpulan dataset untuk pengembangan model deteksi SPAM.
d. Pengujian aplikasi pada tiap event sprint berupa whitebox testing menggunakan unit testing, selanjutnya pengujian blackbox testing dengan application / integration testing dilakukan pada event sprint review di akhir sebuah iterasi pengembangan. Selain itu, khusus pada komponen model generator dilakukan pengujian validasi akurasi menggunakan K-Fold cross validation dan confussion matrix.

2.2 Sumber dan Jenis Data

Terdapat dua jenis data yang digunakan pada penelitian ini yaitu data sekunder dan data primer. Data sekunder yang digunakan meliputi data kualitatif yang didapatkan dari studi literatur tentang pencegahan SPAM, cara penggunaan DNSBL, serta implementasi SVM untuk mendeteksi SPAM. Beberapa hasil dari studi literatur ini antara lain, didapatkannya beberapa sumber DNSBL yang dapat digunakan untuk memvalidasi domain dan IP *origin* pengirim surel serta cara penggunaan DNSBL tersebut. Data sekunder lain yang digunakan pada penelitian ini adalah dataset surel SPAM & HAM yang didapatkan dari data public di Kaggle yang terdiri dari 2551 dokumen HAM dan 501 dokumen SPAM.

Data primer yang digunakan pada penelitian ini adalah hasil pengujian perangkat lunak baik pengujian whitebox menggunakan unit testing, maupun pengujian blackbox dengan pengujian aplikasi terintegrasi seperti pengecekan proses scraping dan proses cek DNSBL. Selain itu data primer lain yang digunakan adalah data hasil pengujian performa dengan menggunakan K-Fold Cross Validation dan Confussion Matrix. Data tersebut untuk memvalidasi apakah model pendeteksi yang dikembangkan sudah layak digunakan atau tidak.

Sesuai tahapan penelitian yang telah dijelaskan pada bagian sebelumnya, kerangka kerja yang digunakan menghasilkan 3 artifak utama yang digunakan sebagai referensi penelitian dan pengembangan sistem [10].

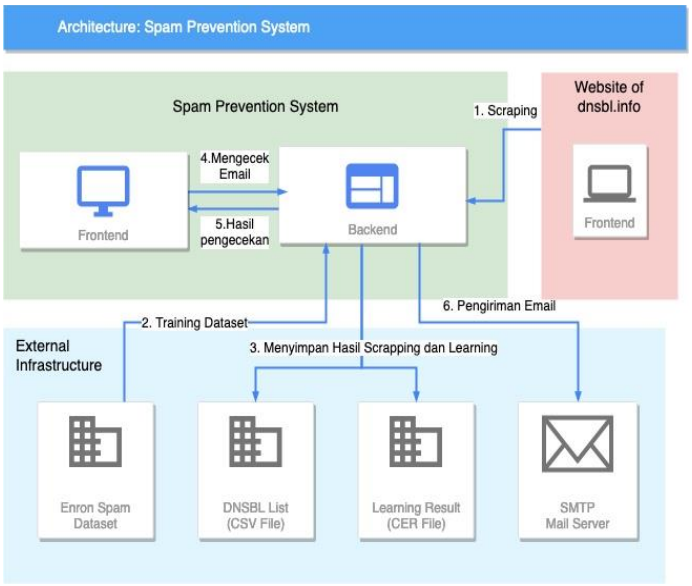
a. Product Backlog, list fitur, pengembangan, dan tugas yang harus dikerjakan untuk mengembangkan sebuah produk / sistem yang diinginkan. Dalam penelitian ini, product backlog didapatkan dari wawancara dengan pemiliki usaha surel marketing dan juga validasi hasil wawancara berdasarkan studi literatur dari beberapa jurnal dengan topik SPAM prevention.
b. Sprint Backlog, kumpulan backlog task yang akan diselesaikan dalam waktu tertentu. Artifact ini dibuat dengan cara memilik beberapa pekerjaan dari product backlog dan memecahnya ke dalam beberapa Sprint Item. Dalam konteks penelitian ini sprint backlog adalah sub sistem independen yang diuji secara terpisah, yaitu komponen Front end, DNSBL scraper, content preprocessor, dan SVM model generator. Keuntungan memecah backlog ke dalam sprint backlog adalah dapat dilakukan pengujian secara lokal tanpa harus menunggu keseluruhan sistem selesai dikembangkan.
c. Product Increment, merupakan customer deliverables yang telah diselesaikan pada tahapan sprint tertentu. Artifak ini berisi dokumen pengembangan aplikasi yang sudah siap digunakan dalam skala kecil, dalam arti pengguna sudah dapat menggunakan produk yang dibuat, dan dapat memberikan feedback kepada pengembang [11].

3. HASIL DAN PEMBAHASAN

3.1 Analisis Arsitektur Sistem

Secara garis besar backend sistem pencegahan SPAM yang dikembangkan terdiri dari dua bagian pokok, yaitu backend untuk generate model deteksi SPAM dan backend untuk mendeteksi SPAM berdasarkan model yang telah dikembangkan. Generator model ini akan melakukan scraping data penyedia DNSBL dari Wikipedia dan dnsbl.info serta menyimpan hasil *scraping* pada basis data internal untuk mendeteksi DNS yang sudah terdeteksi sebagai SPAM sebelumnya. Selain itu, generator model juga menyimpan dataset untuk data training pendeteksi SPAM berbasis konten sesuai langkah yang akan dijelaskan pada bagian selanjutnya. Gambaran dari arsitektur sistem pencegah SPAM yang dikembangkan sebagaimana ditunjukkan pada gambar 2.

Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795

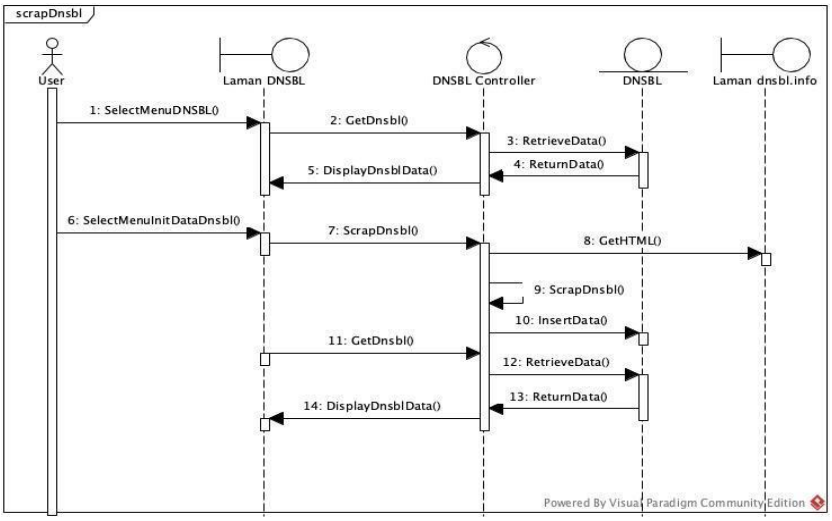


Gambar 2. Arsitektur Sistem Pencegah SPAM

Terlihat pada ilustrasi di Gambar 2, pengguna harus menggunakan *frontend* yang telah disediakan untuk mengecek surel yang akan dikirim, selanjutnya bagian frontend mengirimkan data surel yang akan dikirimkan pada backend untuk dilakukan pengecekan, jika surel yang akan dikirimkan tidak berpotensi menjadi SPAM, backend akan mengirimkan surel tersebut dan menampilkan hasilnya pada pengguna. Sebaliknya, jika surel yang akan dikirimkan terdeteksi berpotensi menjadi SPAM, maka backend akan mencegah pengiriman surel dan memberikan informasi potensi SPAM pada pengguna.

3.2 Analisis Alur *Scrapping* DNSBL

Scraping merupakan proses yang dilakukan untuk mengambil data DNSBL dari laman perbandingan penyedia layanan DNSBL pada laman Wikipedia serta website dnsbl.info [12]. Alur proses *scraping* dimulai dari pengiriman HTTP Request ke laman tersebut secara berkala dan mendapatkan hasilnya dalam format HTML. Selanjutnya dilakukan deteksi pada tag / komponen HTML khusus yang meyimpan data DNSBL, kemudian mengekstraknya ke dalam *array* dan *object* sehingga didapatkan daftar DNSBL. Data yang telah disimpan pada pada *array* tersebut kemudian disimpan kedalam penyimpanan internal jika memang data tersebut belum pernah tersimpan sebelumnya dan akan diabaikan jika data sudah pernah disimpan. Gambaran alur proses *scraping* ini dapat dilihat lebih jelas pada gambar 3.

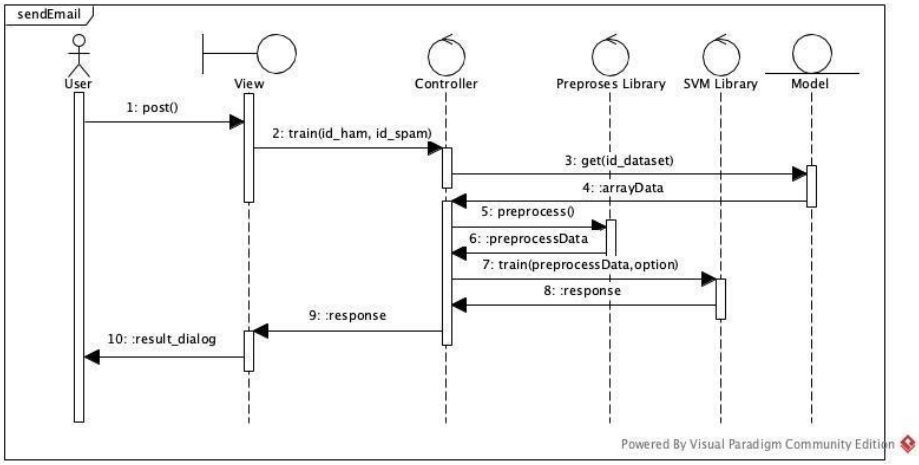


Gambar 3. Sequence Diagram proses Scraping DNSBL

3.3 Analisis Alur *Generate* Model SVM

Proses membuat model yang mendeteksi konten yang berpotensi menjadi SPAM memerlukan dataset yang sudah diberikan label. Selain itu, agar model pendeteksi ini dapat diperbaharui, diperlukan mekanisme untuk menambah dataset dan proses *re-training* dengan dataset terbaru yang lebih banyak dan lengkap. Berdasarkan hal tersebut, sistem yang dikembangkan juga membuat *repository* dataset yang dapat ditambahkan dan diubah oleh admin.

Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795



Gambar 4. *Sequence diagram* proses generate SPAM Detection Model

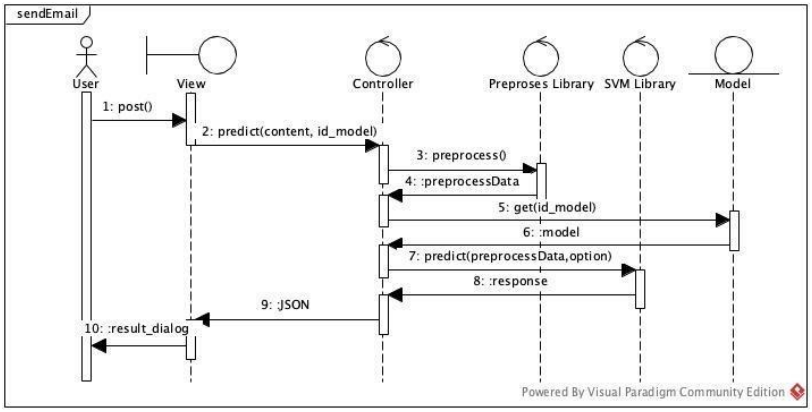
Sebagaimana ditunjukkan pada gambar 4, langkah generate model dimulai dari input dataset yang dapat dilakukan secara massal dengan mengunggah file dataset atau dilakukan secara manual menginputkan data satu-persatu. Selanjutnya, dataset akan dilakukan preproses untuk membersihkan data dan melakukan vektorisasi agar dataset tersebut dapat dibuatkan modelnya. Langkah berikutnya library SVM mengolah dataset yang telah divektorisasi menjadi model agar dapat digunakan untuk pengecekan.

Pada lingkungan produksi, pembuatan model ini tidak hanya dilakukan sekali pada awal saja, namun dapat dilakukan berkali-kali terutama ketika terdapat dataset baru untuk kalibrasi model, sehingga diperlukan mekanisme untuk memperbaharui model berdasarkan pembaruan dataset. Hal tersebut telah ditunjukkan pada Gambar 4, di mana setelah proses modelling terdapat inputan dataset serta re-training model kembali.

Terakhir model yang dihasilkan dari proses training menggunakan SVM disimpan ke dalam sebuah file *.pkl untuk dapat digunakan pada proses pengecekan konten surel. Penyimpanan dalam file *.pkl juga memungkin membuat beberapa versi model untuk untuk kebutuhan versioning dan cadangan jika proses generate model baru terjadi kegagalan atau degradasi akurasi.

3.4 Analisis Alur Pengecekan Surel

Proses pengecekan surel dilakukan tepat sebelum surel dikirim. Ketika pengguna klik tombol kirim, aplikasi akan melakukan pengecekan berdasarkan DNSBL dan model klasifikasi SVM yang telah di-generate sebelumnya. Alur pengecekan surel sebagaimana ditampilkan pada sequence diagram di gambar 6 akan dijelaskan lebih lengkap sebagai berikut.



Gambar 5. Proses generate SVM Model

Langkah pertama, ketika User mengirim surel dari aplikasi Frontend, Backend akan membaca domain dari alamat surel pengirim. Selanjutnya, backend akan melakukan pengecekan menggunakan DNSBL Filter, apabila terdeteksi sebagai SPAM maka akan ditampilkan pesan ke pengguna melalui frontend, dan sebaliknya jika tidak proses akan lanjut ke tahap berikutnya.

Langkah pengecekan selanjutnya adalah pengecekan konten surel, di sini backend akan membaca konten surel dan melakukan stemming, tokenisasi dan stop word removal pada konten surel. Setelah konten surel dibersihkan, barulah backend engine akan melakukan prediksi menggunakan model SVM Filter yang sudah di-generate sebelumnya. Apabila konten diklasifikasikan sebagai spam maka pengguna akan mendapat notifikasi yang ditampilkan melalui Fronten, dan sebaliknya jika tidak lanjut ke tahap berikutnya.

Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795

Setelah proses pengecekan surel selesai, backend akan mengeluarkan dokumen yang berisi hasil pengecekan. Dari hasil tersebut user dapat menentukan apakah surel tersebut layak untuk di kirim atau direvisi.

3.5 Implementasi Preproses Data

Sebagaimana ditampilkan pada gambar 4, Proses pertama yang dilakukan adalah membaca semua dataset yang ada pada repository ke dalam memory untuk persiapan pengolahan. Dataset yang telah tersimpan sudah dikategorikan menjadi dua berdasarkan labelnya yaitu HAM (surel *legitimate*) dan surel SPAM. Selanjutnya semua data yang tersimpan pada memori dilakukan tokenisasi dan *stopword removal* pada tahapan preproses. Ilustrasi sumber dan hasil setelah tahapan preproses dapat dilihat pada tabel 1.

Tabel 1. Contoh text surel sebelum dan setelah preproses

Label	Text	Setelah Preproses
HAM	tw deal analysis - basis differential michelle, the changes for tw deal analysis to use latest basis differential based on receipt point area is in production. thanks, mei-ling	tw, deal, analysis, basis, differential, michelle, changes, tw, deal, analysis, use, latest, basis, differential, based, receipt, point, area, production, thanks, mei, ling.
HAM	transportation contract # 25374 michelle, please ammend oneok buston processings transportation contract # 25374 to include the month of january, 2001. thank you, andrew Pacheco	transportation, contract, michelle, ammend, oneok, buston, processings, transportation, contract, include, month, january, thank, andrew, pacheco.
SPAM	the original your woman needs an 8 inch man. be that man for her. learn how here. turn off notifications here. df international exports ltd st. lina # 8777 belize city, belize	original, woman, needs, inch, man, man, learn, turn, notifications, df, international, exports, ltd, st, lina, belize, city, belize.
SPAM	you'll need this hello, if you want that roock harrd john son check out the first and original one on the market don't be fooled by imitations and copy - cats. later, romero	hello, want, roock, harrd, john, son, check, out, original, market, don't, fooled, imitations, copy, cats, later, romero.

Setelah dilakukan preproses dan tokenisasi, semua kata yang terekam diubah menjadi index dan dilakukan *one hot encoding* terhadap semua kata pada *document dataset* yang tersedia. Pada tahap ini akan didapatkan jumlah fitur yang sangat besar, sehingga berpotensi memperlambat proses *training* [13]. Untuk mengatasi hal tersebut, digunakan Chi Square untuk seleksi fitur, sesuai dengan formula yang ditampilkan pada persamaan (1).

$$X^{c2} = \sum E_i(O_i - E_i)2 \quad (1)$$

Chi square dapat digunakan untuk menentukan *score critical values* untuk masing-masing fitur [14], sehingga selanjutnya fitur yang telah terseleksi dapat dilakukan pembobotan dengan menggunakan *term frequency-inverse document frequency* (TF-IDF) untuk mendapatkan nilai relevansi sebuah term (fitur) terhadap dokumen yang tersedia. TF-IDF dapat dihitung dengan menggunakan fungsi

$$tf\ idf\ (t,d,D) = tf\ (t,d)\ .idf\ (t,D) \quad (2)$$

Di mana:

$$tf\ (t,d) = \log(1 + freq\ (t,d)) \quad (3)$$

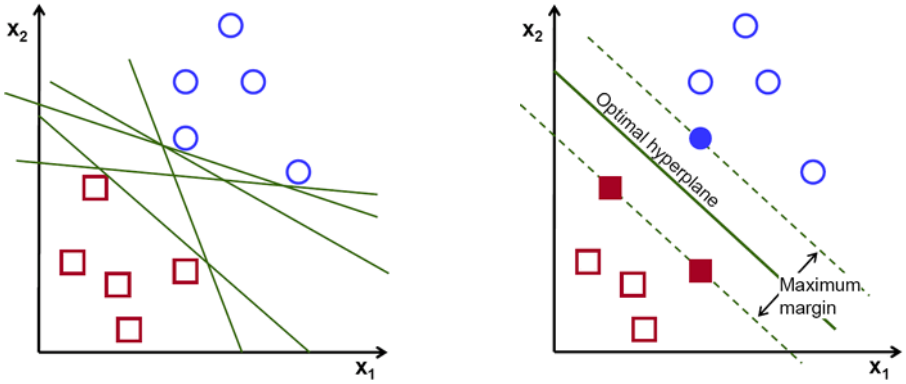
$$idf\ (t,D) = \log(\frac{N}{count\ (d \in D : t \in d)}) \quad (4)$$

Hasil dari TF-IDF tersebut akan didapatkan fitur yang memiliki bobot tinggi dan kemungkinan berpengaruh terhadap dokumen dataset, serta fitur yang memiliki korelasi rendah akan diabaikan untuk mengurangi bias dan meningkatkan akurasi [15].

3.6 Implementasi Modelling dan Evaluasi Model

Tahap terakhir dari proses *modelling* adalah membuat model dari data yang telah di-preproses sebelumnya. Algoritma yang digunakan untuk klasifikasi adalah Support Vector Machine (SVM). Algoritma ini dapat mencari *optimal hyperplane* yang memisahkan input data ke dalam dua set yang berbeda berdasarkan fitur yang telah direduksi dan diberikan bobot sebelumnya. SVM dapat digunakan untuk pekerjaan regresi dan klasifikasi, namun lebih seringnya digunakan untuk tujuan klasifikasi, dengan membuat N-dimensional hyperplane yang secara optimal memisahkan data ke dalam dua kategori [7]. Pada gambar 6 ditampilkan contoh bagaimana SVM dapat menentukan optimal hyperplan dengan fitur terdekat yang merupakan *support vector* pada data 2 dimensi.

Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795



Gambar 6. Penentuan optimal hyperplane dan maximum margin pada SVM

Sebagai catatan, kita tidak dapat menggambarkan *hyperplane* dari implementasi proses modelling deteksi SPAM ini karena ukuran jumlah dimensinya setelah diseleksi menggunakan Chi-Square masih mencapai ratusan. Sebagai gantinya, pada implementasi penelitian ini dilakukan evaluasi terhadap model yang telah dibuat.

Evaluasi dilakukan untuk mengetahui apakah aplikasi yang dibangun dapat berjalan dengan baik dan memenuhi spesifikasi yang ditentukan. Penelitian ini menggunakan metode whitebox dengan menggunakan unit testing untuk memastikan alur logika aplikasi sudah berjalan sesuai kebutuhan, serta blackbox untuk menguji aplikasi secara keseluruha.. Pengujian ini dilakukan pada bagian fungsi-fungsi utama dengan memasukan inputan ke setiap endpoint dan membandingkannya dengan luaran yang dibutuhkan. Beberapa komponen yang akan diuji adalah fungsi pengecekan domain, fungsi scrapping, penambahan, pengurangan serta penambilan DNSBL, training dataset, pengecekan konten spam, dan mengirim surel. Unit testing dilakukan menggunakan JUnit, unit testing framework yang banyak digunakna pada bahasa pemrograman yang menggunakan Java Virtual Machine (JVM) seperti Java dan Kotlin [16]. Hasil dari uji blackbox dan whitebox tidak dapat ditampilkan pada makalah ini karena berupa list skenario uji yang sangat panjang.

Selain pengujian fungsionalitas aplikasi, pada penelitian ini juga dilakukan uji akurasi model menggunakan 10-fold cross validation dan confusion matrix [17] dengan rumus sebagaimana ditunjukkan pada persamaan (5).

$$ACC = \frac{TP+TN}{P+N} = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

Dataset yang dimiliki akan dipecah secara acak menjadi dua kelompok yaitu data training sebesar 80% dan data testing sebesar 20%, selanjutnya proses dilakukan berulang sebanyak 10 kali untuk mendapatkan rata-rata akurasi pengujian. Hasil dari cross validasi tersebut didapatkan nilai sebagai ditampilkan pada table 2, dan dari hasil tersebut dapat disimpulkan model yang digunakan untuk klasifikasi untuk SPAM prevention sudah cukup reliable karena sudah mencapai rata-rata akurasi 97.54%.

Tabel 2. Hasil validasi akurasi model yang dibuat

K	Akurasi	Akurasi Validasi
1	0.8282	0.9599
2	0.9717	0.9799
3	0.9819	0.9774
4	0.9845	0.9724
5	0.9858	0.9774
6	0.9903	0.9825
7	0.9987	0.9724
8	0.9929	0.9774
9	0.9969	0.9749
10	0.9991	0.9799
Rata-rata		0.9754

4. KESIMPULAN

Sistem peringatan dini untuk mendeteksi surel SPAM berbasis DNSBL dan Support Vector Machine (SVM) telah berhasil dikembangkan dan dapat digunakan dengan baik. Sistem peringatan dini ini dapat digunakan oleh organisasi yang menerapkan surel marketing untuk memastikan surel yang dikirim tidak mengalami bounce yang berpotensi merugikan organisasi tersebut. Proses deteksi SPAM dilakukan dalam dua tahap, yaitu mengecek alamat domain dengan DNSBL dan mengecek konten surel dengan model yang dikembangkan menggunakan SVM. Model yang dikembangkan telah divalidasi dengan 10-fold cross validation dan memiliki rata-rata akurasi

Journal of Information System Research (JOSH)
Volume 3, No. 4, Juli 2022, pp 618−625
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v3i4.1795

97.54%, sehingga cukup valid untuk digunakan pada SPAM detection and prevention system. Sistem yang dikembangkan pada penelitian ini telah diuji dan dapat digunakan dengan baik dan dapat digunakan sebagai solusi permasalahan deteksi dini SPAM berbasis *Reputation Filtering* dan *Content Filtering*. Meski demikian ada beberapa hal yang menjadi catatan dan dapat dikembangkan untuk penelitian selanjutnya, pertama data DNSBL yang digunakan sangat bergantung dengan data yang dibuat oleh pihak ketiga, pada penelitian selanjutnya bisa difokuskan untuk mendeteksi dan mendapatkan DNSBL secara mandiri. Pengembangan DNSBL ini dapat dilakukan dengan membuat bot agent yang dapat mendeteksi DNSBL secara mandiri. Kekurangan yang kedua, dataset yang digunakan pada penelitian ini adalah dataset berbahasa inggris, sehinga sebaiknya pada penelitian selanjutnya perlu dilakukan pengembangan dataset SPAM dalam Bahasa Indonesia untuk meningkatkan validitas deteksi pada surel berbahasa Indonesia. Salah satu metode yang dapat digunakan untuk mengembangkan dataset SPAM adalah pengumpulan dataset berbasis crowdsource, sehingga banyak kontributor pihak ketiga yang dapat menyumbang dataset untuk memperkaya deteksi SPAM.

REFERENCES

[1] M. Hartemo, “Email marketing in the era of the empowered consumer,” *J. Res. Interact. Mark.*, 2016.
[2] N. S. Sahni, S. C. Wheeler, and P. Chintagunta, “Personalization in email marketing: The role of noninformative advertising content,” *Mark. Sci.*, vol. 37, no. 2, pp. 236–258, 2018.
[3] D. S. Silnov, “An analysis of modern approaches to the delivery of unwanted emails (spam),” *Indian J. Sci. Technol.*, vol. 9, no. 4, pp. 1–4, 2016, doi: 10.17485/ijst/2016/v9i4/84803.
[4] H. S. Alkahtani, P. Gardner-Stephen, and R. Goodwin, “A TAXONOMY OF EMAIL SPAM FILTERS,” p. 6.
[5] A. Al Mugni, M. F. Herdiansah, M. G. Andhika, and M. Ridwan, “DNSBL for internet content filtering utilizing pfsense as the next generation of opensource firewall,” in *2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2019, pp. 117–121.
[6] E. Blanzieri and A. Bryl, “A survey of learning-based techniques of email spam filtering,” *Artif. Intell. Rev.*, vol. 29, no. 1, pp. 63–92, 2008.
[7] S. Suthaharan, “Support vector machine,” in *Machine learning models and algorithms for big data classification*, Springer, 2016, pp. 207–235.
[8] A. N. Pour, “Minimizing the Time of Spam Mail Detection by Relocating Filtering System to the Sender Mail Server,” *Int. J. Netw. Secur. Its Appl.*, vol. 4, no. 2, pp. 53–62, Mar. 2012, doi: 10.5121/ijnsa.2012.4204.
[9] M. B. Firdaus, I. M. Patulak, A. Tejawati, A. Bryantama, G. M. Putra, and H. S. Pakpahan, “Agile-scrum software development monitoring system,” in *2019 International Conference on Electrical, Electronics and Information Engineering (ICEEIE)*, 2019, vol. 6, pp. 288–293.
[10] F. M. Fowler, “Scrum artifacts,” in *Navigating Hybrid Scrum Environments*, Springer, 2019, pp. 55–57.
[11] F. Dobrigkeit, D. de Paula, and M. Uflacker, “InnoDev: a software development methodology integrating design thinking, scrum and lean startup,” in *Design Thinking Research*, Springer, 2019, pp. 199–227.
[12] M. Fejrskov, J. M. Pedersen, and E. Vasilomanolakis, “Using NetFlow to Measure the Impact of Deploying DNS-based Blacklists,” in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2021, vol. 398 LNICST, pp. 476–496. doi: 10.1007/978-3-030-90019-9_24.
[13] D. Pandya, “Spam Detection Using Clustering-Based SVM,” in *Proceedings of the 2019 2nd International Conference on Machine Learning and Machine Intelligence*, 2019, pp. 12–15.
[14] A. W. Haryanto, E. K. Mawardi, and others, “Influence of word normalization and chi-squared feature selection on support vector machine (svm) text classification,” in *2018 International Seminar on Application for Technology of Information and Communication*, 2018, pp. 229–233.
[15] S. M. H. Dadgar, M. S. Araghi, and M. M. Farahani, “A novel text mining approach based on TF-IDF and Support Vector Machine for news classification,” in *2016 IEEE International Conference on Engineering and Technology (ICETECH)*, 2016, pp. 112–116.
[16] C. Wiecher, J. Greenyer, and J. Korte, “Test-driven scenario specification of automotive software components,” in *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, 2019, pp. 12–17.
[17] S. Yadav and S. Shukla, “Analysis of k-fold cross-validation over hold-out validation on colossal datasets for quality classification,” in *2016 IEEE 6th International conference on advanced computing (IACC)*, 2016, pp. 78–83.