Nama :

1. Futra Sanjaya Hutasoit
2. Muhammad Iman Rizqullah
3. Muhammad Riza Nugroho

**Email Hoax Detection System Using Levenshtein Distance Method**

1. **Masalah**

Hoax email diketahui tidak berbahaya terhadap sistem yang dibuat. Hoax dianggap sebagai sampah yang dapat memberikan informasi menyesatkan kepada pengguna atau pembaca email. Menurut Blanzieri dan Bryl [1], spam adalah surat sampah yang sebagian besar tidak diinginkan atau tidak diminta yang dikirim baik secara langsung maupun tidak langsung oleh personel yang tidak memiliki hubungan saat ini dengan pengguna email. Hoax adalah email yang tidak diminta dan tidak diinginkan yang secara langsung atau tidak langsung dikirim oleh personel yang memiliki hubungan saat ini dengan pengguna email [2]. Singkatnya, hoax adalah spam versi 'pintar' yang menyamar dengan baik melalui personel yang hadir sebagai kontak seseorang. Biasanya hoax datang dalam bentuk penerusan pesan dari berbagai sumber. Informasi menyesatkan dari hoax dapat menyebabkan kerugian finansial dan menjengkelkan pengguna individu. Lebih buruk lagi, tipuan memiliki kemampuan untuk mengumpulkan informasi dan mungkin dapat meyakinkan penerima email untuk bertindak atas peristiwa yang tidak ada.

Beberapa email hoax telah menimbulkan banyak false alarm yang berdampak negatif bagi pihak-pihak tertentu. Misalnya, PayPal harus merusak dan mengambil tanggung jawab setelah penipuan Nigeria yang dianggap sebagai jenis tipuan diteruskan ke sebagian besar penerimanya oleh sumber yang tidak dikenal yang menyamar dengan menggunakan alamat email yang mirip dengan PayPal pada tahun 2003. Kepalsuan lainnya Kewaspadaan akan adanya hujan asam akibat ledakan reaktor nuklir di Jepang juga sempat menimbulkan kekacauan di Asia Tenggara dimana hoax ini diteruskan ke banyak orang setelah seminggu dari kejadian gempa di Jepang. Meskipun hoax ini belum terbukti sebagai penipuan, isinya menyesatkan [2-4].

Meskipun beberapa e-mail hoaks tidak berbahaya, namun seringkali meresahkan masyarakat. Lebih jauh, berdasarkan teori Meme [5], ketika pikiran seseorang terinfeksi oleh informasi yang salah, akan sulit bagi orang yang terinfeksi untuk diyakinkan sebaliknya tentang kebenaran yang sebenarnya. Masalahnya hanya dapat diselesaikan setelah pengguna terpapar pada fakta sebenarnya dari tipuan ini. Meskipun demikian, tidak akan mudah untuk meyakinkan seseorang tentang kebenaran yang hakiki kecuali jika sumber kebenaran yang dikemukakan itu sahih menurut pandangan orang tersebut [5]. Oleh karena itu, hoaks sangat penting untuk diidentifikasi terutama untuk menghindari kesalahpahaman lebih lanjut yang dapat membawa kerugian yang signifikan serta dampak negatif bagi pertumbuhan suatu partai.

Berkaitan dengan hal tersebut, pengembangan sistem pendeteksi hoax secara otomatis bertujuan untuk melindungi penerima email dari penyesatan informasi palsu. Dalam literatur, belum banyak sistem pendeteksi hoax yang dibuat selama ini. Pekerjaan yang terkait dengan sistem deteksi email hoax dinyatakan dalam [2-4]. Sebagian besar pola deteksinya sama tetapi berbeda menurut definisi [1].

1. **Metode**
2. **Sistem Arsitektur**

Sistem deteksi hoax yang diusulkan terdiri dari tiga komponen utama: pra-pemrosesan teks, deteksi hoax dan deteksi hoax baru. Pra-pemrosesan teks mengumpulkan email untuk diuji validitasnya menjadi email asli atau tipuan. Header dan tanda tangan email akan dihapus dari email asli. Sistem menggunakan Levenshtein Distance untuk mengidentifikasi potensi hoax dari konten email dengan membandingkannya dengan database hoax. Basis data hoax terdiri dari email hoax yang dikumpulkan dari Hoax-Slayers.com, yang diakui oleh Perpustakaan Nasional Australia (PANDORA) sebagai sumber hoax yang baik.

1. **Jarak Levenshtein**

Levenshtein Distance (LD) adalah metrik untuk mengukur jumlah perbedaan antara dua string.

Jarak antar string diukur dengan jumlah penyisipan, penghapusan atau penggantian yang diperlukan untuk mengubah string s menjadi string t. Sebagai contoh:

* Jika string sumber (s) "tebal" dan string target (t) juga "tebal", maka LD(s,t) = 0, karena tidak diperlukan transformasi. String identik satu sama lain.
* Jika string sumber asli (s) "tebal" dan string target (t) adalah "bonk", maka LD(s,t) = 2, karena dua substitusi (perubahan "l" menjadi "n" dan "d menjadi “k”) diperlukan untuk mengubah string asli menjadi string yang dibandingkan.

Oleh karena itu, semakin tinggi jarak Levenshtein, semakin berbeda stringnya dan semakin kecil kemungkinan email itu hoax. Isi email yang diinput oleh pengguna akan diperlakukan sebagai string sumber dan string target adalah email hoax yang disimpan dalam database hoax. Hitungan jarak akhir akan diubah menjadi persentase menggunakan rumus berikut:

**Jarak = (100 – jumlah jarak total) \* 100**

Seperti yang telah disebutkan di bagian sebelumnya, sebagian besar sistem pendeteksi hoax yang disebutkan dalam literatur tidak mampu mendeteksi hoax baru. Untuk mengatasi masalah ini, sistem yang diusulkan menambahkan komponen lain untuk mengidentifikasi potensi hoax baru. Oleh karena itu, aturan berikut diterapkan dalam sistem.

1. Jarak lebih besar dari 60%, email adalah kebohongan

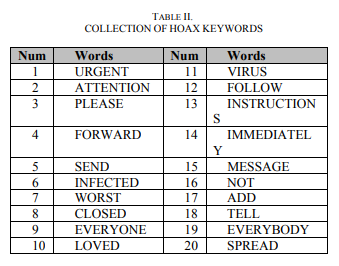
Jarak kurang dari 60%, emailnya adalah diduga hoax. Isi email akan dikirim untuk penyaringan akhir.

1. **Penyaringan Akhir**

Berdasarkan pengamatan kami, hoax memiliki pola serupa yang mudah dideteksi seperti:

* Sering menggunakan huruf besar
* Judul terdiri dari kata-kata seperti URGENT! Mohon FORWARD pesan ini dan lain-lain
* Termasuk kata-kata ekstrim seperti TERBURUK, SANGAT SERIUS dan lain-lain

Kami menyimpan sekantong kata-kata yang terdiri dari kata-kata umum yang sering ditemukan di email hoax. Tabel II adalah kumpulan sampel kantong kata-kata yang ditemukan dari hoax.



Oleh karena itu, kami menghitung persentase kata yang ditulis dalam huruf besar atas jumlah total karakter yang ditemukan dalam email.

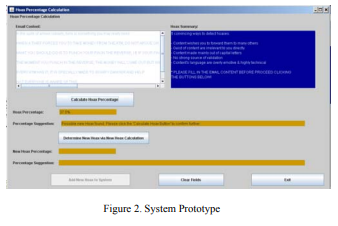
*Persentase Huruf Besar = (Jumlah Total Huruf Besar Karakter / Jumlah Karakter dalam email) \* 100*

*Kata Kunci Persentase = (Jumlah Kata Kunci ditemukan / Jumlah kata dalam email) \* 100*

Kami menerapkan aturan 60% yang disebutkan di atas pada rumus untuk menentukan apakah email tersebut baru atau tidak tipuan email. Hoax email baru yang teridentifikasi akan ditambahkan ke dalam database hoax.

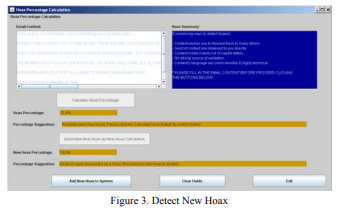
1. **Hasil dan Pembahasan**
2. **Prototipe Sistem**

Seperti ditunjukkan pada Gambar. 2, pengguna yang ingin menguji apakah konten email adalah tipuan perlu menyalin email konten ke sistem. Setelah pengguna mengklik 'Hitung' Tombol Persentase Hoax, level mencurigakan tipuan akan dihitung. Jika level mencurigakan kurang dari 60%, sistem akan menyarankan pengguna untuk menentukan apakah ada tipuan baru terdeteksi.



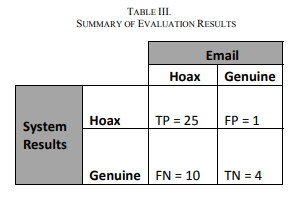
Dalam kasus ketika sistem menyarankan untuk menentukan apakah tipuan baru terdeteksi, pengguna diminta untuk mengklik Dalam kasus ketika sistem menyarankan untuk menentukan apakah tipuan baru terdeteksi, pengguna diminta untuk mengklik tentang ‘Menentukan Hoax Baru melalui Perhitungan Hoax Baru’ tombol. Setelah diklik, level mencurigakan tipuan baru akan dihitung. Seperti yang ditunjukkan pada Gambar. 3, tingkat mencurigakan tipuan adalah 74%. Oleh karena itu, tipuan baru telah terdeteksi dan

konten email akan ditambahkan ke database hoax.



1. **Sistem Evaluasi**

Keakuratan sistem dalam mengidentifikasi email hoax perlu dinilai untuk memastikan sistem yang diusulkan efektif dalam mengidentifikasi email hoax. Ukuran kinerja yang digunakan untuk mengevaluasi keakuratan sistem adalah nilai prediksi positif, nilai prediksi negatif, sensitivitas dan spesifisitas. Sebanyak 40 sampel email diuji menggunakan sistem. Tabel III merangkum hasil evaluasi.



true positive (TP) = email hoax yang benar diidentifikasi oleh system

false positive (FP) = email asli diidentifikasi sebagai email hoax

true negative (TN) = email asli teridentifikasi

false negative (FN) = email hoax diidentifikasi sebagai email asli

Positive Predictive Value (PPV) = TP / (TP + FP)

= 0.96

Negative Predictive Value(NPV) = TN / (FN + TN)

= 0.29

Sensitivity = TP / (TP + FN)

= 0.71

Specificity = TN / (FP + TN)

= 0.80

Nilai prediksi positif yang tinggi (PPV = 0,96) menunjukkan bahwa banyak email hoax yang benar telah diidentifikasi oleh sistem. Nilai prediksi negatif yang rendah (NPV = 0,29) menunjukkan bahwa sistem lemah dalam mengidentifikasi email asli. Oleh karena itu, kemungkinan besar sistem akan memperlakukan email hoax sebagai email asli. Hal ini sesuai dengan nilai sensitivitas yang tinggi (0,71) yang menunjukkan bahwa kemungkinan sistem mengidentifikasi email hoax sebagai email asli tinggi. Sistem memiliki nilai spesifisitas tinggi (0,80); ini menunjukkan bahwa kemungkinan sistem mengidentifikasi email asli sebagai hoax adalah tinggi. Meskipun sistem mampu memberikan hasil yang baik dalam mengidentifikasi email hoax, sistem ini kurang mampu mengidentifikasi email hoax yang ditulis dengan format email asli. Selama pengujian sistem, kami dapat mengamati bahwa sebagian besar email hoax yang telah ditulis secara profesional belum teridentifikasi sebagai hoax oleh sistem. Hal ini karena email yang ditulis secara profesional membantu meningkatkan kepercayaan diri pembaca dan membuat mereka percaya bahwa cerita yang mereka sampaikan adalah benar. Oleh karena itu, dengan menggunakan format email (huruf besar) sebagai salah satu faktor untuk mengidentifikasi email hoax mungkin bukan metode yang mutlak efektif.

1. **Kesimpulan**

Kesadaran akan adanya hoaks menciptakan kesadaran yang lebih besar untuk menemukan pengetahuan yang tepat yang dapat digunakan untuk lebih mengembangkan persepsi manusia saat mereka tumbuh. Informasi yang menyesatkan hanya dapat merugikan kelompok tertentu termasuk mencoreng citra mereka di mata publik. Dalam makalah ini telah dikembangkan sistem pendeteksi hoax dengan menggunakan Levenshtein Distance. E-mail yang diekstraksi dibandingkan dengan database hoax untuk mendukung keputusan identifikasi hoax. Di sisi lain, fitur nilai tambah disarankan dalam sistem yang diusulkan dengan menghadirkan kemungkinan hoaks kepada penerima. Ini membuat perbedaan dari sistem sebelumnya. Sistem ini mampu memberikan nilai prediksi positif tinggi 0,96 tetapi tidak memiliki kemampuan untuk mengidentifikasi email asli. Email hoax tidak hanya dikirim dalam format teks tetapi juga dengan gambar. Koleksi kata kunci hoax terbatas. Oleh karena itu, ini adalah keterbatasan sistem dan masih ada ruang untuk perbaikan.

Untuk pekerjaan di masa depan, sistem dapat ditingkatkan dengan mengintegrasikan teknik kecerdasan buatan seperti logika fuzzy. Dengan teknik ini, sistem seharusnya dapat lebih mengklasifikasikan email hoax dan email asli. Karya-karya sebelumnya dalam pendeteksian hoax tidak mengadopsi teori pemrosesan teks kecuali n-gram. Namun, diyakini bahwa alat penambangan teks lain yang menggunakan algoritma pembelajaran mesin [10] dapat digunakan sebagai pra-pemrosesan teks untuk mengekstrak teks dari email.