JKT Jurnal Komputer Terapan
ISSN : 2443-4159 (Print) ISSN: 2460-5255 (Online)
Politeknik Caltex Riau
Empower You to Global Competition

MEKANISME DETEKSI DAN PEMBLOKIRAN KONTEN PERJUDIAN DARING BERBASIS KATA KUNCI MENGGUNAKAN ALGORITMA LEVENSHTEIN DISTANCE

Ismail Puji Saputra
Teknologi Rekayasa Internet, Politeknik Negeri Lampung, Bandar Lampung, 35141, Indonesia
ismailpujisaputra@gmail.com
**Penulis Koresponden*

ABSTRAK

Perjudian daring (judi online) di Indonesia semakin marak dan menimbulkan dampak negatif, baik dari sisi sosial-ekonomi maupun keamanan siber. Salah satu modus yang digunakan Bandar judi online adalah menyisipkan backlink judi pada website, khususnya domain .ac.id dan .go.id, untuk meningkatkan peringkat pada mesin pencari, Penelitian ini bertujuan membangun mekanisme deteksi dan pemblokiran input berbasis kata kunci guna mencegah penyisipan konten judi daring ke dalam website. Metode yang digunakan yaitu Fuzzy Matching dengan algoritma Levenshtein Distance yang digunakan untuk mengukur tingkat kemiripan antara input pengguna dan kata kunci perjudian. Hasil perhitungan precision sebesar 1.00, recall 0.80, F1-score 0.89, dan akurasi 0.90, hasil ini menunjukan bahwa sistem dapat mendeteksi kalimat yang mengandung unsur perjudian dengan tingkat ketepatan tinggi, namun masih terdapat false negative yang perlu ditingkatkan lagi, sehingga hasil false negative dapat dihindari. Dengan demikian, mekanisme ini dapat menjadi langkah awal dalam upaya pencegahan penyalahgunaan website oleh kelompok kriminal siber.

Kata kunci: *Fuzzy Matching, Keamanan Siber, Judi Online, Levenshtein Distance*

ABSTRACT

Online gambling in Indonesia is increasingly widespread and has negative impacts, both in terms of socio-economic aspects and cybersecurity. One of the methods used by online gambling operators is inserting gambling backlinks into websites, particularly those with .ac.id and .go.id domains, to boost their ranking in search engines. This study aims to develop a keyword-based input detection and blocking mechanism to prevent the insertion of online gambling content into websites. The method employed is Fuzzy Matching with the Levenshtein Distance algorithm, which measures the similarity between user input and gambling-related keywords. The evaluation results show a precision of 1.00, recall of 0.80, F1-score of 0.89, and accuracy of 0.90. These results indicate that the system can detect sentences containing gambling elements with high accuracy; however, false negatives still occur and need further improvement to be minimized. Thus, this mechanism can serve as an initial step in preventing the misuse of websites by cybercriminal groups.

Keywords: *Cybersecurity, Fuzzy Matching, Gambling Online, Levenshtein Distance*

Histori Artikel
Diserahkan: 06 Okt 2025 Diterima setelah Revisi: 27 Okt 2025 Diterbitkan: 29 Nov 2025

1. PENDAHULUAN

Perjudian daring (judi online) semakin marak di Indonesia dan menimbulkan dampak negatif yang signifikan bagi masyarakat. Dampak tersebut tidak hanya terbatas pada aspek ekonomi, tetapi juga merambah ke tatanan sosial [1]. Aktivitas perjudian daring berpotensi menghambat perputaran ekonomi domestik karena sebagian pendapatan masyarakat yang seharusnya digunakan untuk kebutuhan sehari-hari justru dialihkan untuk berjudi[2]. Data transaksi perjudian periode 2017-2023 ditaksir bernilai hingga Rp.200 Triliun[3]. Lebih jauh lagi, praktik perjudian daring turut memicu peningkatan angka kriminalitas akibat individu yang terdesak kebutuhan ekonomi dan memilih jalan pintas melalui tindakan ilegal untuk menutupi kerugian berjudi [4].

Selain menimbulkan dampak sosial-ekonomi, perjudian daring juga terkait erat dengan isu keamanan siber. Dalam memperluas jangkauan, situs perjudian daring umumnya memanfaatkan teknik black SEO melalui kelompok kriminal siber untuk menyusupi website korban[5]. Website sendiri memiliki peran penting dalam ekosistem sistem informasi sehingga kerap menjadi target serangan[6],[7]. Beberapa tahun terakhir, serangan semacam ini banyak ditujukan untuk mengeksploitasi website sebagai media penanaman backlink judi daring, dengan tujuan meningkatkan peringkat situs tertentu pada hasil pencarian mesin pencari, khususnya Google.

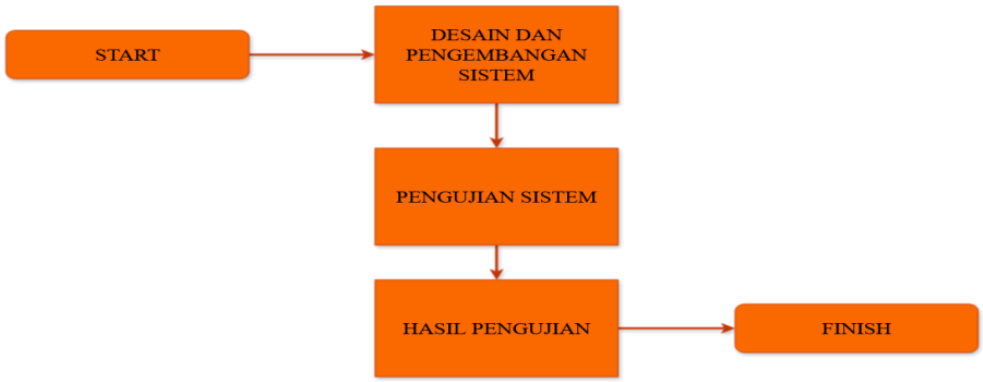
Target utama serangan biasanya adalah website dengan Domain Authority (DA) dan Page Authority (PA) tinggi, seperti domain .ac.id milik institusi pendidikan tinggi atau .go.id milik lembaga pemerintahan. Situs-situs tersebut seringkali memiliki trafik yang besar, tetapi tidak selalu dikelola dengan sistem keamanan yang memadai, sehingga menjadi sasaran strategis bagi kelompok kriminal siber [8]. Fenomena yang marak dewasa ini adalah praktik injeksi atau penyisipan backlink perjudian daring ke dalam website-website tersebut. Hal ini dilakukan untuk menghindari pemblokiran langsung terhadap domain situs perjudian, sekaligus memanfaatkan reputasi website resmi agar kata kunci tertentu muncul di peringkat atas hasil pencarian[9].

Berbagai upaya telah dilakukan untuk mendeteksi serangan semacam ini, namun mekanisme deteksi dan pencegahan yang ada seringkali belum dilakukan ataupun belum cukup efektif, deteksi hanya sebatas mendeteksi dan meneruskan notifikasi kepada administrator [10], hal ini adalah langkah yang dilakukan setelah terjadinya serangan, bukan mencegah serangan, selain itu pembahasan sebatas cara mendeteksi adanya backlink atau tidak, dan bukan mencegah adanya serangan[11]. Dari kasus tersebut fokus penelitian ini adalah untuk membuat mekanisme pemblokiran berbasis kata kunci sehingga serangan dapat dicegah.

Pendekatan yang dilakukan adalah dengan mengumpulkan kata kunci dari mesin pencari Google yang relevan dengan aktivitas perjudian daring, kemudian menggunakan kata kunci tersebut sebagai acuan pencocokan terhadap input pengguna. Jika ditemukan kesesuaian, sistem akan secara otomatis memblokir input tersebut. Selanjutnya, penelitian ini juga menguji tingkat efektivitas mekanisme dengan mengukur persentase keberhasilan pemblokiran terhadap berbagai jenis input. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi pada bidang keamanan siber, khususnya dalam upaya meminimalisasi penyalahgunaan website oleh kelompok kriminal siber yang bergerak di bidang perjudian daring.

2. METODE

Metode penelitian yang dilakukan untuk membangun mekanisme deteksi dan pemblokiran serangan dapat dilihat pada Gambar 1. Alur Penelitian:



Gambar 1. Alur Penelitian

Langkah pertama yang dilakukan adalah desain dan pengembangan sistem, sistem dikembangkan dengan metode *waterfall* yaitu metode pengmbangan yang terstruktur dan berurutan [12]. Pada tahap ini, sistem dirancang dengan memperhatikan kebutuhan deteksi serangan yang berfokus pada penyisipan *backlink* perjudian (gambling *backlink*). Proses pengembangan meliputi perancangan arsitektur sistem, penentuan alur deteksi, serta pembuatan aturan berbasis kata kunci *(keyword-based detection)* yang dikumpulkan dari hasil pencarian pada mesin pencari google. Tujuan dari tahap ini adalah menghasilkan prototipe sistem yang mampu mengenali pola serangan berupa penyisipan konten judi ke dalam *website*,

selain itu sistem ini akan memblokir *input* dari pengguna apabila mengandung *keyword* judi daring yang telah dikumpulkan.

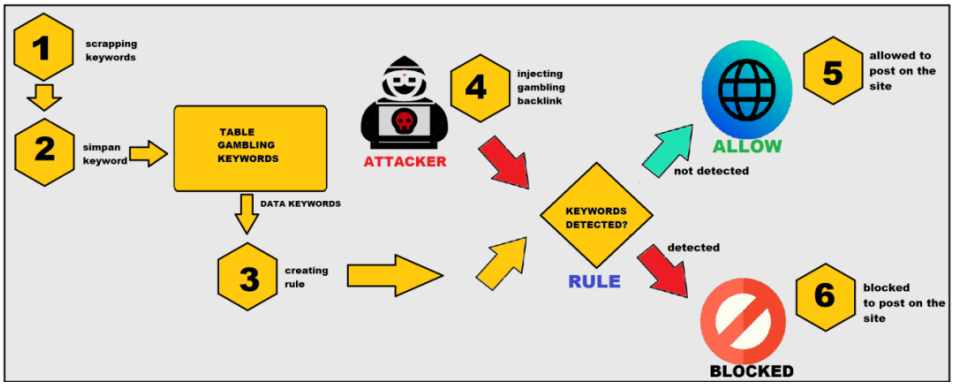
Tahap berikutnya adalah pengujian sistem. Pengujian dilakukan dengan cara memberikan *input* berupa data uji yang terdiri dari teks normal dan teks yang telah disisipi kata kunci perjudian. Pada tahap ini diamati apakah sistem dapat membedakan konten yang bersih dengan konten berbahaya yang mengandung kata-kata terkait perjudian, pengujian ini menghitung akurasi dengan memperhatikan jumlah *false positive* maupun *false negative*, sehingga tingkat kedekatan sistem terhadap nilai sebenarnya dapat diketahui [13].

Tahap terakhir adalah analisis hasil pengujian, hasil uji sistem kemudian disajikan dalam bentuk grafik serta dijelaskan secara deskriptif untuk mengambil kesimpulan dari hasil pengujian[14]. Analisis ini bertujuan untuk mengevaluasi sejauh mana efektivitas sistem dalam melakukan deteksi dan pemblokiran konten berbahaya. Dari hasil analisis tersebut dapat ditarik kesimpulan apakah mekanisme yang dibangun telah sesuai dengan tujuan penelitian atau masih membutuhkan pengembangan lebih lanjut.

3. HASIL DAN PEMBAHASAN

3.1 DESAIN DAN PENGEMBANGAN SISTEM

Hasil desain sistem yang dibangun memiliki cara kerja yang dapat dilihat pada Gambar 2.



Gambar 2. Mekanisme Deteksi

Pada Gambar 2. Mekanisme Deteksi, dapat dijelaskan secara deskriptif sebagai berikut:

i) *Scraping Keyword*
Scraping keyword dilakukan untuk mendapatkan kata kunci yang mengandung judi daring, berikut ini *pseudocode* yang menggambarkan proses *scraping* data *keyword* judi daring:

```
Start
      Dorking google slot gacor site: .ac.id .go.id
      Dorking situs toto togel online site: .ac.id .go.id
 Simpan sebagai $Keyword
Finish
```

ii) Simpan *Keyword*
Setelah *keyword* didapatkan, maka proses selanjutnya adalah menyimpan *keyword*s tersebut kedalam *database* untuk digunakan sebagai pembanding dalam mendeteksi *input* pengguna.

iii) Membuat *rule*
Keywords yang telah disimpan akan dibandingkan dengan *input* pengguna, berikut ini *pseudocode rule* yang akan digunakan untuk mendeteksi dan mengantisipasi serangan:

```
Start
      $Keyword=['keyword ke 1 - keyword ke n'];
      $InputUser=['input user'];
          If{
               $InputUser terdapat $Keyword = Blokir;
            } else
               $InputUser simpan ke database;
Finish
```

iv) *Scanning input* pengguna
Setiap proses *input* pengguna pada suatu *form* akan melalui proses pemeriksaan terlebih dahulu, *input* pengguna akan dicocokan dengan menggunakan metode *Fuzzy Matching* yang dapat mengukur kecocokan antara *string keyword* dan *string input* pengguna [15]. Algoritma yang digunakan pada metode ini menggunakan algoritma Levenshtein Distance yang biasa digunakan untuk mengukur kecocokan suatu kata dengan menghitung jarak antara kedua kata tersebut [16], berikut ini adalah pseudocode langkah pencocokan dari algoritma Levenshtein Distance:

```
Start
$Input: "kucing", "dinding"
    Hitung berapa banyak huruf yang berbeda
    Bandingkan huruf satu per satu dari depan
    k ≠ d → beda +1
    u ≠ i → beda +1
    c ≠ n → beda +1
    i = i → sama
    n = n → sama
    g = g → sama
    (huruf sisa di "dinding" → d,i,n) → tambah beda +3
    $Total_beda = 6
    $Panjang_kata_terpanjang = 7
    $Persentase_kemiripan = (1 - 6/7) × 100% = 14.3%
Finish
```

Implementasi Levenshtein Distance dapat menggunakan *library fuzzywuzzy* dengan menggunakan fungsi *token_set_ratio* yang berfungsi memecah *string* menjadi kata-kata, dan menghitung skor dari kata-kata yang sama [17].

v) Pengambilan Keputusan
Pemblokiran akan dilakukan apabila kecocokan antara *input pengguna* dan *keywords*, sebaliknya apabila antara *input* pengguna dan *keywords* tidak cocok, maka *input* pengguna akan diijinkan untuk masuk kedalam *database*.

3.2 PENGUJIAN SISTEM

Pengujian yang dilakukan menggunakan bahasa pemrograman python yang mencocokan *string keyword*s yang didapatkan dari google yaitu "Situs Slot Gacor Resmi, Situs Togel Online Terpercaya, Slot Gacor, Togel, Maxwin, Slot Gampang Menang" dengan contoh *input* pengguna dapat dilihat pada Tabel 1.

Tabel 1. Hasil Kemiripan String

No	Input User	Kemiripan %
1	Ok88 adalah agen slot gacor viral terbaru yang resmi memberikan kesempatan gampang menang jackpot maxwin, bisa langsung mendadak kaya dan sudah terbukti gacor di seluruh platform Slot Indonesia.	72
2	Ismail ganteng suka mencetak goal, dia sangat gacor mainya di lapangan hari ini, sehingga timnya menang terus.	43
3	main slot gacor gampang menang	91
4	agen togel *online* terpercaya	90
5	maxwin setiap hari	50
6	tim sepak bola menang besar	36
7	ronaldo mainnya gacor, hasilnya timnya menang terus.	53
8	promo diskon belanja *online*	36
9	situs judi slot terpercaya	89
10	belajar matematika *online*	39

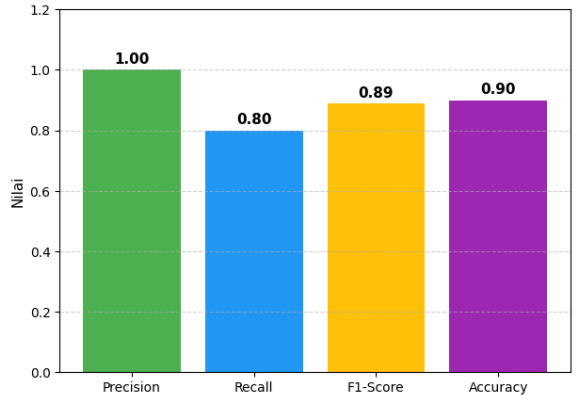
Hasil persentase kemiripan antara *keyword* dan *input* pengguna diuji untuk melihat apakah kalimat diatas diprediksi dengan benar, proses pengujian dilakukan dengan ketentuan ambang batas *(threshold)* yang bernilai 70%, nilai *threshold* 70% dipilih karena nilai tersebut dianggap cukup tinggi untuk menunjukan kemiripan yang kuat namun masih memberikan toleransi terhadap perbedaan kecil seperti

kesalahan ketik ataupun variasi kata. Maka apabila terdapat *input* pengguna yang memiliki kemiripan ≥ 70% akan dilabeli sebagai kalimat yang mengandung perjudian, sedangkan jika kalimat memiliki kemiripan < 70% akan dilabeli bukan kalimat perjudian. Hasil pengujian dari 10 *sample* kalimat dapat dilihat pada tabel 2.

Tabel 2. Hasil Pengujian

No	Kemiripan %	Label Aktual	Label Prediksi	Hasil Prediksi
1	72	Judi	Judi	Benar
2	43	Bukan	Bukan	Benar
3	91	Judi	Judi	Benar
4	90	Judi	Judi	Benar
5	50	Bukan	Judi	Salah
6	36	Bukan	Bukan	Benar
7	53	Bukan	Bukan	Benar
8	36	Bukan	Bukan	Benar
9	89	Judi	Judi	Benar
10	39	Bukan	Bukan	Benar

Berdasarkan Tabel 2, dapat dilihat bahwa dari 10 sampel kalimat, sistem berhasil memprediksi sebagian besar *input* dengan benar, namun masih terdapat kesalahan klasifikasi pada kata nomor 5 dimana seharusnya kalimat "maxwin setiap hari" merupakan kalimat yang biasa dipakai untuk *backlink* judi, namun diprediksi sebagai bukan judi (*false negative*), hal ini karena kalimat terlalu pendek, sehingga pembanding kemiripan *keyword* judi dan bukan *keyword* judi menjadi tidak imbang. Untuk menilai performa sistem secara lebih rinci, hasil prediksi tersebut kemudian dirangkum ke dalam *confusion matrix* sehingga dapat dihitung nilai *precision*, *recall*, *F1-score* dan *accuration* dari model [18]. Berikut ini gambar 3 menunjukkan hasil *confusion matrix*.



Gambar 3. Hasil Confusion Matrix

Berdasarkan Gambar 3 Diatas, dapat dilihat bahwa nilai *precision* 1 yang menandakan bahwa tidak ada *false positive* dalam prediksi, nilai *recall* 0.80 menandakan masih terdapat *false negative*. Nilai *F1-score* dengan nilai 0.89 merupakan hasil rata-rata dari *precision* dan *recall*, sedangkan *Accuration* merupakan hasil dari keberhasilan prediksi yang memiliki nilai 0.90.

4. KESIMPULAN

Berdasarkan hasil pengujian menunjukan bahwa sistem yang dibangun menggunakan metode *Fuzzy Matching* dengan algoritma Levenshtein Distance, mampu mendeteksi *input* pengguna yang terindikasi sebagai kalimat yang mengandung *keyword*s perjudian, khususnya judi daring, serta melakukan pemblokiran pada *input* pengguna, sehingga *input* pengguna tidak masuk kedalam *database*. Namun untuk kasus prediksi dalam konteks keamanan komputer, hasil *false negative* tidak dapat ditoleransi, artinya kalimat yang seharusnya dianggap *keyword*s judi namun dideteksi bukan perjudian, hal ini akan menimbulkan lolosnya kalimat tersebut kedalam *database*, Untuk itu, diperlukan penelitian lanjutan guna mengembangkan metode perhitungan kesamaan teks yang lebih adaptif terhadap variasi panjang kalimat. Pendekatan tersebut diharapkan dapat mengurangi tingkat *false negative*, yaitu kondisi ketika dua teks yang sebenarnya memiliki makna serupa justru diklasifikasikan sebagai tidak mirip akibat keterbatasan algoritma Levenshtein Distance dalam memperhitungkan panjang dan konteks semantik.

UCAPAN TERIMAKASIH
Ucapan terimakasih penulis ucapkan kepada seluruh dosen yang ada pada Program Studi Teknologi Rekayasa Internet, Politeknik Negeri Lampung, motivasi dan dorongan untuk terus meneliti dan berdampak pada masyarakat membuat penulis menjadi semangat dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

[1] S. Sihombing, R. A. M. Sahputri, M. G. Njoman, and L. E. Rini, "Sosialisasi Bahaya JUDOL (Judi Online) Dalam Perspektif Ekonomi di SMKN 2 Sungailiat-Bangka," Jurnal Pengabdian Kepada Masyarakat Politeknik Negeri Batam, vol. 7, no. 1, pp. 38–49, 2025.

[2] S. Afrioza, I. J. Sakti, A. L. Febrianti, R. A. Hamdani, B. Digital, and U. Y. Madani, "Literasi Digital Adaptif Sebagai Strategi Pencegahan Judi Online dan Penguatan Ketahanan Remaja: Studi Kasus di," JEDBUS (Journal of Economic Digital Business), vol. 2, no. 2, pp. 75–84, 2025.

[3] S. Marsela, A. Syifa, F. D. Pratama, and R. Al Muqfi, "Persoalan Perjudian dan Judi Online dalam Analisa Teori Etika Utilitarianisme," Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat, vol. 1, no. 2, pp. 1–20, 2023, doi: 10.11111/dassollen.xxxxxxx.

[4] N. A. Syakira, N. F. Ramadhahana, N. D. Anggita, T. Tsaqifa, and R. N. Husna, "Dampak Konsumerisme Berupa Judi Online di Indonesia: Perspektif Ekonomi, Sosial, dan Mental," Jurnal Interaktif, vol. 16, no. 2, pp. 73–79, 2024, doi: 10.21776/ub.interaktif.2024.016.02.3.

[5] D. H. Hendarto and R. S. Handayani, "Pencegahan Kejahatan Siber Terkait Distribusi Perjudian Online di Indonesia dalam Rangka Mewujudkan Keamanan dan Ketertiban Masyarakat," Jurnal Syntax Admiration, vol. 5, no. 5, pp. 1542–1558, 2024, doi: 10.46799/jsa.v5i5.1136.

[6] D. Supriadi, E. Suryadi, R. Muslim, and L. D. Samsumar, "Implementasi Vulnerability Assessment OWASP (Open Web Application Security Project) pada Website Universitas Teknologi Mataram," Journal of Data Analysis, Information, and Computer Science, vol. 1, no. 4, pp. 232–240, 2024, doi: 10.70248/jdaics.v1i4.1368.

[7] E. S. Alim, N. Nuroji, M. A. Rizkiawan, T. Anhari, and B. Sobari, "Monitoring dan Pencegahan Serangan Judi Online (Slot Gacor) pada Website," Edumatic: Jurnal Pendidikan Informatika, vol. 8, no. 1, pp. 75–83, 2024, doi: 10.29408/edumatic.v8i1.25267.

[8] P. Agustin and A. Wahyu, "Analisis Keamanan Situs '.go.id' terhadap Serangan Web Defacement 'Judi Online'," Search (Informatics, Science, Entrepreneurship, Applied Art, and Research Humanism), vol. 24, no. 1, pp. 1–10, 2025.

[9] D. A. Herawati, A. Risdhianto, and E. Saptono, "Indonesia Darurat Judi Online: Judi Online sebagai Ancaman Nirmiliter terhadap," Jurnal Ilmiah Manajemen dan Informasi, vol. 5, no. 5, pp. 1251–1261, 2025, doi: 10.53866/jimi.v5i5.991.

[10] M. Hikmatyar, A. Sudiarjo, R. Ruuhwan, M. I. Arief, and N. Fadilah, "Pengembangan Aplikasi Scanning Defacement Judi Online untuk Website Profile pada Server," Informatics Digital Expert, vol. 6, no. 2, pp. 171–175, 2024, doi: 10.36423/index.v6i2.2023.

[11] M. Nurseno, U. Aditiawarman, H. A. Q. Maarif, and T. Mantoro, "Detecting Hidden Illegal Online Gambling on .go.id Domains Using Web Scraping Algorithms," MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 23, no. 2, pp. 365–378, 2024, doi: 10.30812/matrik.v23i2.3824.

[12] N. A. Al Azfar and S. D. Anggita, "Penerapan Metode Waterfall pada Sistem Informasi E-Rapor," Information Systems Journal, vol. 7, no. 1, pp. 45–55, 2024, doi: 10.24076/infosjournal.2024v7i01.1582.

[13] R. Antonius, A. R. Zulkarnain, and H. Irsyad, "Pendekatan TF-IDF, SMOTE, dan SVM dalam Klasifikasi Sentimen Masyarakat terhadap Pemblokiran Judi Online," Buletin Ilmiah Informatika dan Teknologi, vol. 2, no. 3, pp. 115–122, 2024, doi: 10.58369/biit.v2i3.65.

[14] M. Waruwu, S. N. Pu'at, P. R. Utami, E. Yanti, and M. Rusydiana, "Metode Penelitian Kuantitatif: Konsep, Jenis, Tahapan dan Kelebihan," Jurnal Ilmiah Profesi Pendidik, vol. 10, no. 1, pp. 917–932, 2025, doi: 10.29303/jipp.v10i1.3057.

[15] A. N. Cahyo, R. Hermawan, M. Avin, and D. Wijaya, "Deteksi Teks Promosi Judi Online pada Kolom Komentar YouTube dengan Metode Regex dan Fuzzy Matching," Jurnal Teknologi Informasi dan Komputer, vol. 7, no. 2, pp. 176–187, 2025.

[16] M. G. Pradana, H. B. Seta, N. Irzavika, P. H. Saputro, and R. Rusiyono, "Levenshtein Distance Algorithm in Javanese Character Translation Machine Based on Optical Character Recognition,"

International Journal of Informatics and Visualization, vol. 9, no. 4, pp. 1411–1418, 2025, doi: 10.62527/joiv.9.4.3151.

[17] Y. D. Putra et al., "Analisa Pencarian dan Pencocokan String dalam Aplikasi Berbasis Python dengan Library Fuzzy Wuzzy terhadap Dataset Email: String Search and Matching Analysis in Python-Based Application with Fuzzy Wuzzy Library on CNN Daily Mail," Jurnal Teknologi dan Komputer, vol. 4, no. 2, pp. 7–13, 2025.

[18] I. Markoulidakis and G. Markoulidakis, "Probabilistic Confusion Matrix: A Novel Method for Machine Learning Algorithm Generalized Performance Analysis," Technologies, vol. 12, no. 7, 2024, doi: 10.3390/technologies12070113.