Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

Klasifikasi Website Phishing Menggunakan Metode X-Gboost dengan Teknik Penyeimbang Data Radial Based Undersampling

Yoga Yoga*, Fajri Rakhmat Umbara, Puspita Nurul Sabrina

Teknik Informatika, Fakultas Sains dan Informatika, Universitas Jenderal Achmad Yani, Cimahi, Indonesia
Email: [1,*]yoga21@if.unjani.ac.id, [2]fajri.rakhmat@lecture.unjani.ac.id, [3]puspita.sabrina@lecture.unjani.ac.id
Email Penulis Korespondensi: yoga21@if.unjani.ac.id
Submitted: **08/07/2025**; Accepted: **01/09/2025**; Published**: 02/09/2025**

Abstrak−Website phishing merupakan salah satu bentuk serangan siber yang marak terjadi dan berpotensi menyebabkan kerugian besar, baik secara finansial maupun non-finansial. Deteksi phishing secara otomatis menggunakan algoritma pembelajaran mesin menjadi solusi yang efektif untuk menangani ancaman ini. Penelitian ini bertujuan untuk mengklasifikasikan website phishing menggunakan algoritma Extreme Gradient Boosting (XGBoost), serta mengatasi masalah ketidakseimbangan data dengan menerapkan metode Radial Based Undersampling (RBU). Selain itu, dilakukan juga proses tuning hyperparameter menggunakan metode Random Search untuk mengoptimalkan kinerja model. Dataset yang digunakan diperoleh dari platform Kaggle dan memiliki distribusi kelas yang tidak seimbang, di mana jumlah data pada kelas non-phishing jauh lebih banyak dibandingkan kelas phishing. Ketidakseimbangan ini dapat menyebabkan model bias dan kurang mampu mengenali pola kelas minoritas. Berdasarkan hasil pengujian, penerapan RBU secara signifikan meningkatkan kemampuan model dalam mendeteksi kelas minoritas, sementara tuning hyperparameter turut menyempurnakan akurasi. Model terbaik dicapai dengan kombinasi RBU dan Random Search, dengan akurasi sebesar 90,39% pada data uji. Hasil penelitian ini menunjukkan bahwa pendekatan gabungan antara penyeimbangan data dan optimasi model memberikan solusi yang efektif dalam klasifikasi website phishing serta dapat diterapkan pada berbagai kasus serupa dalam bidang keamanan siber.

Kata Kunci: Website Phishing; X-gboost; Radial Based Undersampling; Random Search; Data Imbalance

Abstract−Phishing websites are one of the most prevalent forms of cyberattacks and have the potential to cause significant losses, both financially and non-financially. Automatic phishing detection using machine learning algorithms has become an effective solution to address this threat. This study aims to classify phishing websites using the Extreme Gradient Boosting (XGBoost) algorithm and to address the issue of class imbalance by applying the Radial Based Undersampling (RBU) method. In addition, hyperparameter tuning was performed using the Random Search method to optimize the model's performance. The dataset used was obtained from the Kaggle platform and exhibits an imbalanced class distribution, where the number of non-phishing instances far exceeds phishing instances. This imbalance can lead to a biased model and reduce its ability to detect minority class patterns. Based on the evaluation results, the application of RBU significantly improved the model's capability in detecting phishing instances, while hyperparameter tuning further enhanced its accuracy. The best model was achieved through a combination of RBU and Random Search, reaching an accuracy of 90.39% on the test data. These findings indicate that the combined approach of data balancing and model optimization provides an effective solution for phishing website classification and can be applied to similar cases in the field of cybersecurity.

Keywords: Website Phishing; X-gboost; Radial Based Undersampling; Random Search; Data Imbalance

1. PENDAHULUAN

Phishing merupakan salah satu bentuk serangan siber yang dapat menyebabkan kerugian besar, baik bagi individu maupun organisasi perusahaan. Situs web phishing dirancang untuk menipu pengguna dengan berbagai cara, termasuk penggunaan URL yang mencurigakan, sertifikat SSL palsu, atau elemen desain yang menyerupai situs web resmi. Informasi yang biasanya menjadi sasaran meliputi data identitas diri (seperti nama, alamat, jenis kelamin, tanggal lahir), data akun (seperti nama pengguna dan kata sandi), serta informasi keuangan (seperti kartu kredit dan akun) [1]. Dalam konteks ini, pengembangan model pembelajaran mesin untuk mendeteksi phishing secara otomatis menjadi solusi yang sangat diperlukan.

Di Indonesia, lembaga Indonesia Anti Phishing Data Exchange (IDADX) mencatat sebanyak 106.806 laporan serangan phishing sejak tahun 2018. Pada tahun 2023, jumlah serangan mencapai 65.525, dengan jumlah serangan tertinggi terjadi pada Februari 2023, yaitu 15.050, dan jumlah terendah pada November 2023 sebanyak 1.729. Pada kuartal keempat tahun tersebut, tercatat 8.161 serangan yang menggunakan 53 nama domain. Industri yang paling terdampak adalah industri media sosial, yang mencatatkan 64,34% dari total serangan [2]. Selain itu, Federal Bureau of Investigation (FBI) melaporkan pada Maret 2023 bahwa kerugian akibat serangan siber sepanjang tahun 2022 mencapai lebih dari US$10 miliar, yang setara dengan Rp147 triliun. FBI juga mencatat lebih dari 800 ribu pengaduan terkait serangan siber, dan total akumulasi serangan siber dalam lima tahun terakhir mencapai 3,26 juta kasus dengan kerugian total sebesar US$27,6 miliar atau sekitar Rp406 triliun. Angka-angka tersebut mengindikasikan bahwa ancaman phishing tidak hanya berdampak pada kerugian finansial, tetapi juga mengurangi kepercayaan publik terhadap transaksi online, yang pada gilirannya dapat memberikan dampak negatif yang besar pada bisnis [3]. Tingginya jumlah serangan phishing menunjukkan bahwa ancaman ini bersifat serius, menegaskan perlunya sistem deteksi yang lebih canggih untuk melindungi pengguna secara lebih efektif.

Pada penelitian ini, pendekatan yang digunakan untuk mengklasifikasikan situs web phishing adalah dengan menggunakan algoritma yang terbukti efektif dalam menangani masalah klasifikasi dalam berbagai penelitian sebelumnya [4], [5]. Salah satu algoritma yang dipilih untuk tugas ini adalah XGBoost, yang merupakan algoritma

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

boosting berbasis pohon keputusan. XGBoost dikenal dengan kemampuannya dalam menangani dataset besar dan kompleks [6], serta kemampuannya dalam mengidentifikasi pola-pola yang menunjukkan apakah sebuah situs web adalah phishing atau legitimate.

Penelitian ini bertujuan untuk memanfaatkan metode XGBoost dalam mengklasifikasikan website phishing berdasarkan berbagai fitur, seperti panjang URL, keberadaan simbol mencurigakan, jumlah karakter, jumlah pengalihan di URL, serta fitur lainnya yang relevan. Namun, data yang digunakan untuk penelitian ini tidak seimbang antara jumlah data phishing dan legitimate. Ketidakseimbangan ini dapat menyebabkan model tidak dapat belajar dengan baik, sehingga mengurangi akurasi [7]. Di mana pada penelitian lain penggunaan XGBoost dan teknik balancing data menghasilkan akurasi sebesar 0,94 [8]. Oleh karena itu, diperlukan metode untuk menyeimbangkan data, yaitu Radial Based Undersampling. Metode ini dipilih karena kombinasi antara XGBoost dengan Radial Based Undersampling masih belum banyak dieksplorasi dalam penelitian sebelumnya.

Pada penelitian sebelumnya [4], XGBoost terbukti lebih baik dibandingkan metode Random Forest dalam mengklasifikasikan performa keuangan UMKM,dengan akurasi mencapai 0,944 dan F1-score sebesar 0,950. Hal ini menunjukkan bahwa XGBoost tidak hanya memberikan hasil yang lebih baik dalam hal akurasi dan F1-score, tetapi juga memberikan wawasan lebih mendalam terkait faktor yang memengaruhi performa. Selain itu, pada penelitian lainnya [5], algoritma XGBoost berhasil mengklasifikasikan status kelulusan mahasiswa dengan presisi sebesar 88,89%. Kemudian hasil serupa pada penelitian [9], yang menggabungkan algoritma XGBoost dengan teknik penyeimbang data SMOTETomek dalam mendeteksi situs phishing berhasil mencapai akurasi sebersar 97,8%.

Namun, berdasarkan studi sebelumnya [10], pendekatan yang digunakan masih terbatas pada Support Vector Machines, Decision Trees, dan Long Short-Term Memory Networks. Penelitian ini belum mengeksplorasi efektivitas XGBoost dalam klasifikasi website phishing. Selain itu, penelitian sebelumnya menghadapi kendala seperti akurasi yang kurang optimal, waktu pelatihan yang lama, serta kesulitan dalam menangani data yang tidak seimbang, yang dapat menyebabkan bias dalam prediksi. Oleh karena itu, penelitian ini bertujuan untuk menganalisis kinerja XGBoost dalam klasifikasi website phishing serta mengombinasikannya dengan metode Radial Based Undersampling untuk menangani ketidakseimbangan data.

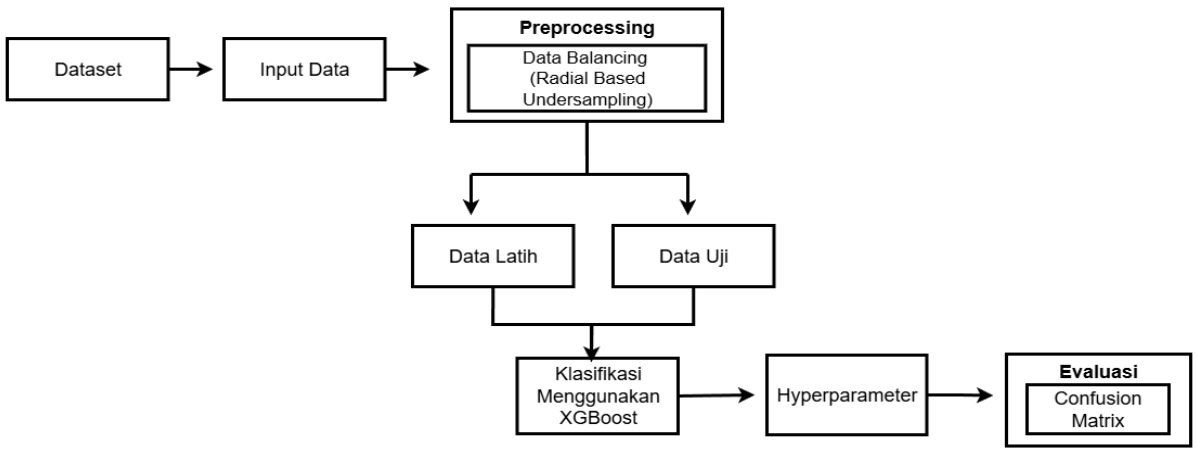
Selain penanganan data tidak seimbang, penelitian ini juga mengkaji efektivitas metode tuning hyperparameter dalam meningkatkan performa model klasifikasi. Salah satu teknik yang digunakan adalah Random Search, yang dikenal efisien dalam menemukan kombinasi hyperparameter optimal tanpa harus menjelajahi seluruh ruang pencarian. Dengan mengimplementasikan Random Search, diharapkan model XGBoost dapat menghasilkan akurasi, presisi, recall, dan F1-score yang lebih optimal. Evaluasi ini penting untuk memastikan bahwa model tidak hanya seimbang dalam mengenali kelas minoritas, tetapi juga memiliki kemampuan generalisasi yang baik terhadap data baru dan tidak terlatih sebelumnya.

Melalui penelitian ini, diharapkan dapat dihasilkan model klasifikasi yang mampu mendeteksi website phishing secara lebih akurat. Selain memberikan kontribusi ilmiah, penelitian ini juga bertujuan meningkatkan kesadaran masyarakat terhadap pentingnya keamanan siber, serta mendorong organisasi untuk mengimplementasikan sistem deteksi phishing yang efektif.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Berikut adalah alur metode penelitian berdasarkan penelitian [11], Proses ini dilakukan untuk Klasifikasi website phishing menggunakan metode XGBoost dengan tek penyeimbang data Radial Based Undersampling yang ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Penelitian

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

2.2 Dataset

Pada tahap awal penelitian ini adalah mengindentifikasi dan menyiapkan objek penelitian berupa data website phishing. Dataset yang digunakan adalah Web Page Phishing Dataset yang tersedia di platform Kaggle oleh Daniel Fernando (https://www.kaggle.com/datasets/danielfernandon/web-page-phishing-dataset). Dataset ini memiliki 100077 record dan 20 atribut, dengan disribusi kelas yang tidak seimbang jumlah data legimate lebih jauh banyak dibandingkan dengan data phishing. Hal ini menjadikan dataset ini relevan sebagai objek penelitian untuk menguji efektivitas algoritma klasifikasi, khususnya dalam konteks data tidak seimbang, fokus penelitian ini yaitu mengklasifikasikan website phishing secara akurat dengan memanfaatkan metode XGBoost, serta mengatasi ketidakseimbangan kelas melalui pendekatan Radial Based Undersampling.

2.3 Input Data

Setelah data terkumpul, langkah selanjutnya adalah melakukan input data ke dalam sistem yang akan digunakan untuk analisis. Data yang telah dikumpulkan akan diorganisir dan dimasukkan ke dalam format yang sesuai untuk pemrosesan lebih lanjut. Penting untuk memastikan bahwa data yang diinput telah melalui verifikasi untuk menghindari kesalahan yang dapat mempengaruhi hasil analisis.

2.4 Preprocessing Data

Sebelum dataset digunakan untuk melatih model, diperlukan penyesuaian data terlebih dahulu guna memastikan bahwa kualitas data tidak memengaruhi kinerja model secara buruk [12], Preprocessing merupakan tahap penting yang bertujuan untuk mempersiapkan data agar siap digunakan dalam pemodelan. Pada penelitian ini, data yang digunakan mengalami ketidakseimbangan kelas, yang dapat menyebabkan model lebih cenderung memprediksi kelas mayoritas dibandingkan kelas minoritas. Untuk mengatasi masalah ini, metode Radial Based Undersampling digunakan. RBU menggunakan konsep potensi kelas mutual, yang sebelumnya diterapkan dalam Radial-Based Oversampling (RBO), untuk memandu proses pengambilan sampel dalam prosedur undersampling [13]. Algoritma ini menentukan urutan pengurangan objek mayoritas berdasarkan seberapa besar kontribusi mereka terhadap potensi kelas mutual, sehingga objek yang kurang berkontribusi dapat dihapus terlebih dahulu.

$$\Phi(x,K,\kappa,\gamma) = \sum_{i=1}^{|K|} exp\left(-\left(\frac{\|K_i - x\|}{\gamma}\right)^2\right) - \sum_{j=1}^{|\kappa|} exp\left(-\left(\frac{\|\kappa_j - x\|}{\gamma}\right)^2\right) \quad (1)$$

Pada persamaan (1), Φ(x, K, κ, γ) disebut sebagai mutual class potential, yaitu fungsi yang mengukur sejauh mana titik x “berpihak” pada kelas mayoritas atau minoritas. Dalam fungsi ini K merupakan himpunan objek dari kelas mayoritas, sementara κ himpunan objek dari kelas minoritas. lalu γ parameter yang mengontrol "cakupan" dari fungsi basis radial (RBF). Selain itu ‖Ki − x‖² dan ‖κj − x‖² menyatakan jarak kuadrat antara titik uji x dan masing-masing anggota dari kelas mayoritas dan minoritas.

2.5 Pembagian Data

Pada tahap ini, data yang telah melalui proses preprocessing dibagi menjadi dua bagian, yaitu data pelatihan dan data pengujian. Proses pembagian dilakukan dengan proporsi 70% data untuk pelatihan dan 30% data untuk pengujian. . Pada tahap ini, data pelatihan digunakan untuk membangun model atau pola, sementara data pengujian digunakan untuk menguji kinerja model yang telah dibentuk [14]. Pembagian ini bertujuan untuk memastikan bahwa model dapat diuji menggunakan data yang belum pernah dilihat sebelumnya, sehingga hasil evaluasi lebih objektif.

2.6 Model X-GBoost

Pada tahap ini, peneliti akan membangun model klasifikasi menggunakan algoritma XGBoost. XGBoost bekerja dengan membangun model prediksi melalui kombinasi beberapa pohon keputusan (decision trees) secara berurutan. (XGBoost) bekerja layaknya metode boosting lainnya, yaitu dengan menggabungkan beberapa model klasifikasi lemah menjadi satu model yang lebih kuat. Proses pelatihannya dilakukan secara bertahap, di mana setiap model baru dilatih berdasarkan kesalahan (residual atau error) dari model sebelumnya [15]. Pohon-pohon dalam kumpulan tersebut dirancang sedemikian rupa agar dapat mendekati nilai residu dari prediksi sebelumnya semaksimal mungkin. Konsep ini dijelaskan dalam rumus berikut [16].

$$\hat{y}_i = \sum_{k=1}^{K} f_k(x_i), f_k \in F \quad (2)$$

$\hat{y}_i$ adalah nilai dari prediksi, F adalah himpunan yang mencakup seluruh pohon regresi, f_k yaitu salah dari pohon regresi dan K adalah jumlah total dari pohon regresi.

Karakteristik utama dari fungsi objektif adalah bahwa fungsi tersebut terdiri dari dua komponen utama: kerugian pelatihan (training loss) dan regularisasi [17].

$$obj\ (\theta) = L(\theta) + \Omega(\theta) \quad (3)$$

L adalah fungsi *training loss*, dan Ω yaitu fungsi *regularization* dan θ parameter berupa model terkait. *training loss* yaitu untuk mengukur seberapa prediktif model terkait dengan data pelatihan

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

2.7 Hyperparameter

Pada tahap ini dilakukan proses tuning hyperparameter, Hyperparameter merupakan parameter yang ditentukan sebelum proses pelatihan model dimulai dan tidak dipelajari langsung dari data. Optimasi hyperparameter merupakan proses penyetelan nilai-nilai hyperparameter pada suatu algoritma guna memperoleh performa terbaik. Setiap algoritma memiliki jenis hyperparameter yang berbeda-beda [18]. Pada tahap ini tuning parameter dilakukan menggunakan Random Search, dimana random serach bekerja dengan memilih sejumlah kombinasi parameter secara acak dari ruang parameter yang tersedia. Metode ini lebih menekankan pada eksplorasi parameter-parameter yang diperkirakan memiliki pengaruh besar terhadap kinerja model [19].

2.8 Evaluasi Model

Setelah pemodelan menggunakan xgboost dilakukan evaluasi model menggunakan confusion matrix, Confusion matrix merupakan alat untuk mengevaluasi kinerja suatu model klasifikasi dalam membedakan data dari berbagai kelas. Jika model berhasil mengklasifikasikan data dengan benar, maka hasilnya disebut True Positive atau True Negative. Sebaliknya, jika terjadi kesalahan dalam pengklasifikasian, maka akan menghasilkan False Positive atau False Negative [20]. Confusion matrix adalah table yang digunakan untuk menilai kinerja model klasifikasi, dengan menunjukan jumlah objek yang diprediksi dengan benar dan yang salah. Confusion matrix mencakup beberapa perhitungan :

a. Presisi
   Presisi merupakan metrik yang digunakan untuk mengukur proporsi data yang benar-benar termasuk kategori positif dari seluruh data yang diprediksi sebagai positif. Nilai presisi dapat dihitung menggunakan rumus pada persamaan berikut [21].

$$Presisi = \frac{TP}{FN+TP} \quad (4)$$

b. Recall
   Recall adalah metrik yang digunakan untuk mengukur proporsi data yang berhasil diprediksi sebagai positif dengan benar dibandingkan dengan seluruh data yang sebenarnya termasuk kategori positif. Nilai recall dapat dihitung menggunakan rumus pada persamaan berikut.

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

c. F1 Score
   F1 Score merupakan metrik yang digunakan untuk menghitung rata-rata harmonis antara presisi dan recall. Nilai F1 Score dihitung menggunakan rumus yang ditampilkan pada persamaan berikut.

$$F1\,Score = 2 \times \frac{Recall \times Presisi}{Recall + Presisi} \quad (6)$$

d. Akurasi
   Akurasi ialah metrik untuk mengukur sejauh mana model dapat melakukan klasifikasi dengan benar. Perhitungan akurasi dapat dilakukan menggunakan Persamaan berikut.

$$Akurasi = \frac{TN+TP}{TP+TN+FP+FN} \quad (7)$$

Keterangan : True Positive (TP) menunjukkan jumlah sampel positif yang berhasil diklasifikasikan dengan benar oleh model. False Positive (FP) menggambarkan jumlah sampel negatif yang keliru diprediksi sebagai positif. False Negative (FN) merujuk pada jumlah sampel positif yang salah diklasifikasikan sebagai negatif. Sementara itu, True Negative (TN) adalah jumlah sampel negatif yang berhasil diprediksi dengan tepat sebagai negatif oleh model [22].

3. HASIL DAN PEMBAHASAN

3.1 Dataset

Dataset yang digunakan dalam penelitian ini adalah Web Page Phishing Dataset yang diperoleh dari platform Kaggle. Dataset ini dirancang untuk membantu proses klasifikasi antara situs web yang tergolong phishing dan situs yang tergolong aman (legitimate). Secara keseluruhan, dataset ini memuat 100.077 record, di mana setiap record merepresentasikan satu halaman web dengan serangkaian informasi berbasis URL. Tujuan utama dari penggunaan dataset ini yaitu untuk membangun model klasifikasi yang mampu membedakan secara otomatis antara halaman phishing dan non-phishing berdasarkan ciri khas dari URL-nya. Penggunaan dataset ini sangat penting karena dalam dunia nyata, serangan phishing menjadi salah satu ancaman siber yang paling umum dan merugikan, terutama bagi pengguna internet yang awam.

Setiap record dilengkapi dengan 20 atribut fitur yang menggambarkan karakteristik teknis dari URL. Beberapa di antaranya adalah url_length, yaitu panjang keseluruhan URL, yang bisa menunjukkan kompleksitas atau upaya

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

penyamaran situs phishing. Lalu ada n_dots (jumlah titik dalam URL) dan n_hypens (jumlah tanda hubung), yang kerap digunakan untuk memecah atau menyamarkan nama domain. n_underline dan n_slash masing-masing mencatat jumlah garis bawah dan garis miring yang ada dalam struktur URL. Fitur-fitur ini sangat penting karena banyak situs phishing mencoba meniru URL resmi dengan menambahkan simbol-simbol atau karakter yang tampak mirip.

Atribut lainnya seperti n_questionmark, n_equal, dan n_and mencerminkan jumlah karakter khusus yang biasanya digunakan dalam parameter URL. Sementara itu, karakter-karakter seperti @, !, *, #, dan $ juga dicatat melalui atribut n_at, n_exclamation, n_asterisk, n_hastag, dan n_dollar, karena sering dijumpai pada URL palsu yang mencoba memanipulasi tampilan atau struktur link. Fitur n_space, n_tilde, n_comma, n_plus, dan n_percent juga dimasukkan untuk menangkap keberadaan karakter non-alfabet yang tidak umum digunakan pada URL sah. Atribut-atribut ini tidak hanya berfungsi sebagai fitur input, tetapi juga memberikan insight tentang bagaimana penyerang mendesain link palsu untuk menipu korban. Terakhir, n_redirection mencatat jumlah pengalihan yang ada dalam URL, karena situs phishing sering menggunakan redirect ke domain yang berbeda untuk mengelabui pengguna.

Label klasifikasi ditandai dengan atribut phishing, di mana nilai 1 berarti phishing dan 0 berarti aman. Meskipun begitu, distribusi kelas dalam dataset ini tidak seimbang. Kelas non-phishing jauh lebih dominan dibanding phishing. Ketidakseimbangan ini berisiko menyebabkan bias pada model, sehingga diperlukan proses penyeimbangan data agar model dapat belajar secara adil dan akurat dalam mengenali kedua kelas. Penyeimbangan ini penting dilakukan untuk memastikan performa model tetap optimal dan tidak hanya mengandalkan mayoritas data. Seperti ditunjukkan Gambar 2, tampilan awal dataset menampilkan data yang akan digunakan.

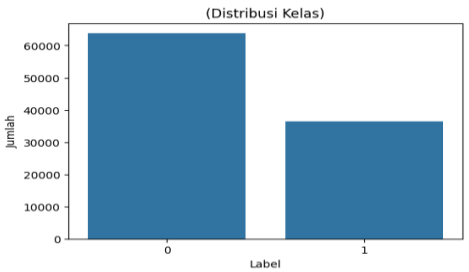
	url_length	n_dots	n_hypens	n_underline	n_slash	n_questionmark	n_equal	n_at	n_and	n_exclamation	n_space	n_tilde	n_comma	n_plus
0	37	3	0	0	0	0	0	0	0	0	0	0	0	0
1	77	1	0	0	0	0	0	0	0	0	0	0	0	0
2	126	4	1	2	0	1	3	0	2	0	0	0	0	0
3	18	2	0	0	0	0	0	0	0	0	0	0	0	0
4	55	2	2	0	0	0	0	0	0	0	0	0	0	0
5	32	3	1	0	0	0	0	0	0	0	0	0	0	0
6	19	2	0	0	0	0	0	0	0	0	0	0	0	0
7	81	2	0	0	0	0	0	0	0	0	0	0	0	0
8	42	2	0	0	0	0	0	0	0	0	0	0	0	0
9	104	1	10	0	0	0	0	0	0	0	0	0	0	0

Gambar 2. Dataset Penelitian

3.2 Preprocessing Data

Pada tahap preprocessing data dalam penelitian ini, salah satu langkah penting yang dilakukan adalah menangani masalah ketidakseimbangan kelas dalam dataset. Hal ini terjadi karena jumlah data pada kelas mayoritas (non-phishing) jauh lebih banyak dibandingkan dengan kelas minoritas (phishing). Ketidakseimbangan seperti ini dapat menimbulkan bias dalam proses pelatihan model, di mana model cenderung belajar lebih banyak dari kelas mayoritas dan mengabaikan pola dari kelas minoritas. Hal ini tentu sangat tidak ideal, terutama dalam konteks deteksi phishing, karena dapat menyebabkan model gagal mengenali situs phishing yang sebenarnya sangat penting untuk dideteksi secara akurat demi menjaga keamanan pengguna.

Untuk mengatasi masalah tersebut, penelitian ini menggunakan metode Radial Based Undersampling (RBU). RBU merupakan salah satu teknik undersampling yang bertujuan untuk mengurangi jumlah data pada kelas mayoritas. Tidak seperti metode Random undersampling yang bekerja dengan cara menghapus data secara acak, RBU melakukan pengurangan data secara lebih cerdas dan selektif dengan mempertimbangkan jarak spasial antar data. Data yang terlalu dekat atau tidak memberikan kontribusi variasi informasi yang signifikan akan dihapus, sementara data penting tetap dipertahankan. Dengan pendekatan ini, RBU mampu menjaga keberagaman informasi pada kelas mayoritas meskipun sebagian besar datanya telah dikurangi. Gambar 3 memperlihatkan ketidakseimbangan yang cukup signifikan antara jumlah data phishing dan non-phishing.

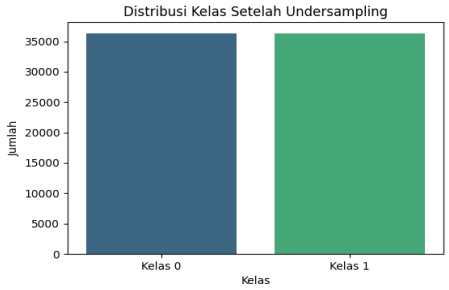


Gambar 3. Distribusi Kelas Awal

Dalam implementasinya, RBU dijalankan menggunakan parameter gamma sebesar 0.001 dan rasio sampling 1.0. Parameter gamma digunakan untuk mengatur ambang jarak antar data, sehingga hanya data yang benar-benar

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

redundan yang akan dihapus. Sementara itu, rasio 1.0 menandakan bahwa jumlah data yang dihasilkan pada kelas mayoritas akan disesuaikan sepenuhnya dengan jumlah data pada kelas minoritas, sehingga keduanya menjadi seimbang. Dengan kombinasi parameter ini, proses undersampling menghasilkan distribusi akhir yang sangat ideal, Gambar 4 menunjukan distribusi kelas yang sudah seimbang, di mana jumlah data untuk kelas 0 (non-phishing) dan kelas 1 (phishing) masing-masing adalah 36.362 record.



Gambar 4. Distribusi kelas setelah RBU

Dengan distribusi yang seimbang tersebut, model pembelajaran mesin yang digunakan dalam penelitian ini dapat belajar dari kedua kelas secara adil. Upaya ini dilakukan untuk memastikan bahwa model tidak berat sebelah dan mampu mengidentifikasi baik situs phishing maupun non-phishing dengan tingkat akurasi yang baik dan konsisten. Selain itu, proses penyeimbangan ini juga membantu meningkatkan kemampuan generalisasi model, sehingga performa deteksi phishing dapat tetap optimal ketika diaplikasikan pada data baru di dunia nyata yang beragam dan dinamis. Oleh karena itu, langkah preprocessing ini menjadi fondasi utama dalam menghasilkan model yang handal dan efektif dalam mendukung keamanan siber.

3.3 Model XGBoost

Model klasifikasi dalam penelitian ini dikembangkan menggunakan algoritma Extreme Gradient Boosting, yang lebih dikenal dengan sebutan XGBoost. Algoritma ini dipilih karena kemampuannya yang sangat baik dalam menangani dataset yang besar dan kompleks, serta kecepatan dan akurasi yang tinggi dalam proses pelatihan model. XGBoost juga memiliki mekanisme regularisasi yang membantu mengurangi risiko overfitting, sehingga model yang dihasilkan lebih mampu melakukan generalisasi pada data baru. Untuk mendapatkan performa terbaik dari model ini, dilakukan serangkaian eksperimen dengan tiga skenario utama, yang bertujuan untuk membandingkan hasil pelatihan dan pengujian model dengan kondisi data yang berbeda.

Skenario pertama adalah pelatihan dan pengujian model XGBoost menggunakan data asli tanpa melakukan penyeimbangan. Pada tahap ini, model dilatih dengan dataset yang tidak seimbang, di mana jumlah data pada kelas non-phishing jauh lebih banyak dibandingkan dengan kelas phishing. Kondisi ini seringkali menyebabkan model lebih condong mempelajari pola dari kelas mayoritas sehingga mengabaikan kelas minoritas. Meskipun begitu, hasil evaluasi pada data latih menunjukkan akurasi yang cukup tinggi, yaitu sebesar 90,19%. Lalu diuji pada data uji yang juga tidak seimbang menghasilkan akurasi 89,47%. Hal ini mengindikasikan bahwa model masih memiliki keterbatasan dalam mengenali pola dari kelas phishing yang jumlahnya lebih sedikit.

Skenario kedua dilakukan dengan menerapkan penyeimbangan data menggunakan teknik Radial Based Undersampling (RBU) sebelum melatih model XGBoost. Dengan metode ini, jumlah data pada kelas mayoritas dikurangi secara selektif sehingga menjadi seimbang dengan kelas minoritas. Penyeimbangan ini bertujuan agar model dapat belajar dengan lebih adil dari kedua kelas tanpa bias. Setelah proses penyeimbangan, model dilatih kembali dan hasil evaluasi menunjukkan peningkatan performa yang cukup signifikan. Akurasi pada data latih meningkat menjadi 91,11%, sedangkan pada data uji juga mengalami peningkatan menjadi 90,33%. Peningkatan ini menandakan bahwa penyeimbangan data berhasil membantu model dalam mengenali pola-pola phishing dengan lebih baik, sehingga prediksi yang dihasilkan menjadi lebih akurat dan dapat diandalkan.

Secara keseluruhan, eksperimen ini menunjukkan bahwa penggunaan teknik penyeimbangan data seperti RBU sangat penting dalam pengembangan model deteksi phishing. Dengan data yang seimbang, model XGBoost dapat bekerja secara optimal dan memberikan hasil yang lebih konsisten dalam membedakan situs phishing dan non-phishing. Hal ini tentu sangat bermanfaat dalam upaya meningkatkan keamanan dunia maya dan melindungi pengguna dari ancaman phishing yang semakin berkembang.

3.4 Hyperparameter

Setelah proses pelatihan model XGBoost dasar selesai dilakukan, langkah penting berikutnya dalam penelitian ini adalah melakukan tuning hyperparameter guna mengoptimalkan performa model. Tuning hyperparameter adalah proses penyesuaian nilai-nilai parameter tertentu yang secara langsung memengaruhi cara kerja model. Tujuannya adalah agar model dapat memberikan hasil prediksi yang lebih akurat, stabil, dan tidak overfitting. Dalam penelitian ini, metode yang digunakan untuk tuning adalah Random Search, yaitu metode pencarian parameter terbaik dengan menguji kombinasi nilai-nilai secara acak dalam ruang pencarian yang telah ditentukan sebelumnya.

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

Random Search dipilih karena mampu mengeksplorasi ruang parameter secara efisien tanpa harus mencoba seluruh kemungkinan kombinasi yang tersedia, seperti yang dilakukan pada Grid Search. Dalam praktiknya, berbagai kombinasi nilai hyperparameter dicoba, dan performanya dievaluasi berdasarkan hasil akurasi pada data latih dan data uji. Hasil terbaik kemudian dipilih untuk digunakan dalam pelatihan akhir model. Metode ini sangat efektif untuk menemukan konfigurasi yang optimal dalam waktu yang relatif singkat, sehingga proses pengembangan model menjadi lebih efisien. Tabel 1 Menyajikan kombinasi nilai-nilai hyperparameter terbaik hasil pemilihan metode random search, Nilai dari hyperparameter terbaik tersebut dapat dilihat pada tabel berikut ini.

Tabel 1. Hyperparameter Terbaik

Hyperparameter	Random Search Values	Nilai Parameter terbaik
max_depth	3, 6, 9, 12	12
learning_rate	0.1, 0.2, 0.3, 0.4, 0.5	0.3
n_estimators	200, 300, 400, 450, 500	300
Gamma	0, 0.1, 0.3, 0.5, 0.7	0.5
Subsample	0.6, 0.7, 0.8, 0.9, 1.0	1.0
min_child_weight	1, 3, 5	1

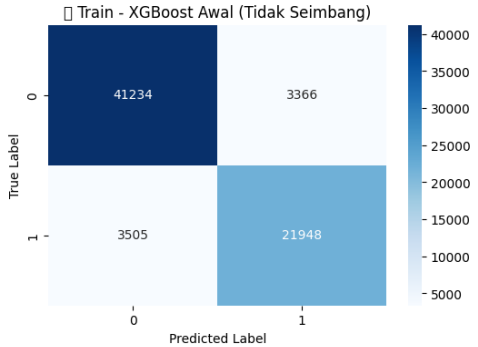
Pemilihan nilai-nilai tersebut menunjukkan bahwa model yang lebih dalam (depth = 12) dan lebih agresif dalam pembelajaran (learning_rate 0.3), dikombinasikan dengan jumlah estimator yang tidak terlalu tinggi, menghasilkan performa optimal untuk dataset ini. Parameter gamma yang cukup besar juga membantu model dalam mengontrol kompleksitas dan mengurangi risiko overfitting, sedangkan subsample penuh memastikan model belajar dari keseluruhan data yang tersedia.

Proses tuning ini kemudian diuji dalam dua skenario. Pertama, model dituning menggunakan data tidak seimbang (tanpa penyeimbangan). Hasilnya, model menghasilkan akurasi sebesar 0.9061 pada data latih dan 0.8952 pada data uji. Kedua, tuning dilakukan pada data yang telah diseimbangkan dengan metode RBU (Radial Based Undersampling). Hasilnya jauh lebih baik, dengan akurasi 0.9156 pada data latih dan 0.9039 pada data uji. Peningkatan ini menunjukkan bahwa penyeimbangan data sangat berpengaruh terhadap kemampuan model dalam mengenali pola dari kedua kelas secara seimbang.Perbandingan hasil dari kedua skenario tersebut menunjukkan bahwa tuning hyperparameter lebih optimal jika dilakukan pada data yang telah seimbang. Model tidak hanya menjadi lebih akurat, tetapi juga lebih stabil dalam mengenali pola dari kedua kelas, baik phishing maupun non-phishing. Dengan demikian, kombinasi antara penyeimbangan data dan tuning hyperparameter terbukti memberikan hasil terbaik dalam penelitian ini, sekaligus meningkatkan keandalan model dalam mendeteksi ancaman phishing secara efektif di dunia nyata.

3.5 Evaluasi Model

Untuk mengevaluasi kinerja dari setiap model yang dibangun, penelitian ini menggunakan analisis metrik klasifikasi yang diperoleh dari confusion matrix, termasuk accuracy, precision, recall, dan F1-score. Evaluasi dilakukan pada empat model yang dikembangkan dari kombinasi kondisi data dan proses tuning yang berbeda. Langkah ini bertujuan untuk melihat bagaimana pengaruh penyeimbangan data dan tuning hyperparameter terhadap performa model XGBoost.

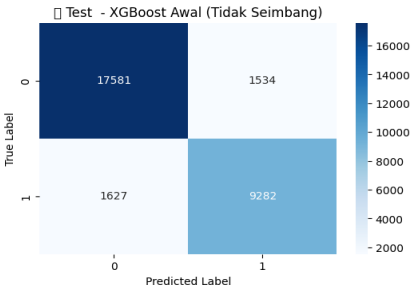
a. Model XGBoost Awal (Tanpa Penyeimbangan Data)
   Model pertama adalah model dasar yang dilatih menggunakan data tidak seimbang, yakni data asli tanpa proses penyeimbangan. Tujuan dari skenario ini adalah untuk mengetahui performa awal model sebelum dilakukan perbaikan pada distribusi data. Hasil evaluasi menunjukkan bahwa akurasi pada data latih sebesar 0.9019, dan pada data uji sebesar 0.8947. Nilai precision, recall, dan F1-score juga berada pada kisaran yang sama, yakni sekitar 0.8945 hingga 0.9019. Meskipun hasil ini cukup baik, namun karena model belajar dari data yang tidak seimbang, dikhawatirkan model lebih fokus pada pola kelas mayoritas saja. Gambar 5 menampilkan performa model XGBoost saat dilatih menggunakan data yang belum seimbang.



Gambar 5. Train - XGBoost Awal (Tidak Seimbang)

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

Kemudian seperti terlihat pada Gambar 6 menunjukan hasil pengujian dari model XGBoost yang dilatih tanpa proses penyeimbangan.



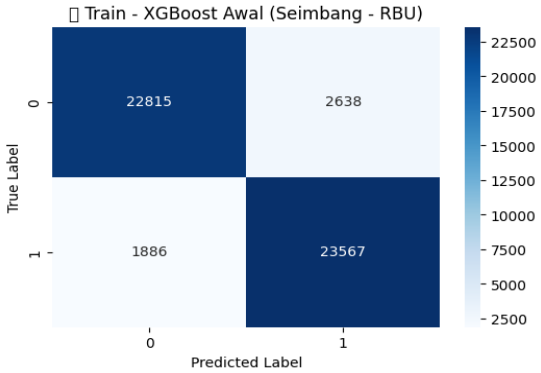
Gambar 6. Test - XGBoost Awal (Tidak Seimbang)

Untuk melihat performa model secara numerik, berikut disajikan tabel seperti pada tabel 2 , yaitu metrik evaluasi yang meliputi accuracy, precision, recall, dan F1-score baik pada data train maupun test. :

Tabel 2. Model XGBoost Awal Data Tidak Seimbang

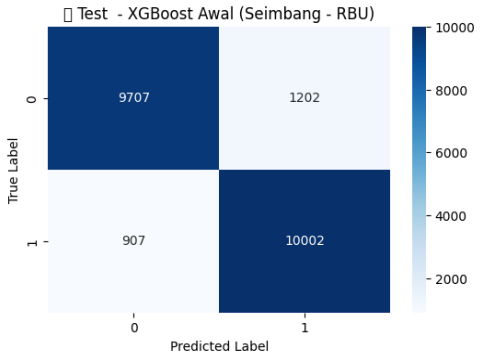
Evaluasi.	Train	Test
Accuracy	0.9019	0.8947
Precision	0.9018	0.8945
Recall	0.9019	0.8947
F1-Score	0.9019	0.8946

b. Model XGBoost (Dengan Penyeimbangan Data RBU)
Model kedua dilatih menggunakan data yang telah diseimbangkan dengan metode Radial Based Undersampling (RBU). Teknik ini membantu menyeimbangkan distribusi antara kelas phishing dan non-phishing, sehingga model belajar secara adil dari kedua kelas. Seperti pada Gambar 7 hasilnya menunjukkan peningkatan performa yang cukup signifikan, dengan akurasi pada data latih mencapai 0.9111 dan akurasi pada data uji sebesar 0.9033. Semua metrik lainnya pun meningkat secara konsisten.



Gambar 7. Train-XGBoost Awal (Seimbang - RBU)

Kemudian seperti terlihat pada Gambar 8, model yang di uji dengan data seimbang menunjukkan hasil yang lebih akurat dan proporsional dibandingkan model sebelumnya



Gambar 8. Test - XGBoost Awal (Seimbang - RBU)

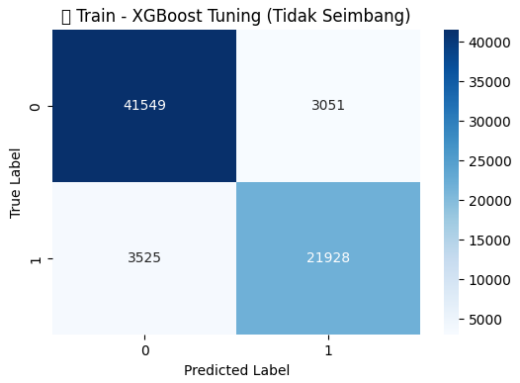
Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

Berikut disajikan Tabel 3, yaitu tabel evaluasi model untuk melihat pengaruh penyeimbangan data terhadap kinerja metrik klasifikasi seperti accuracy, precision, recall, dan F1-score. :

Tabel 3. Model XGBoost Awal Data Seimbang

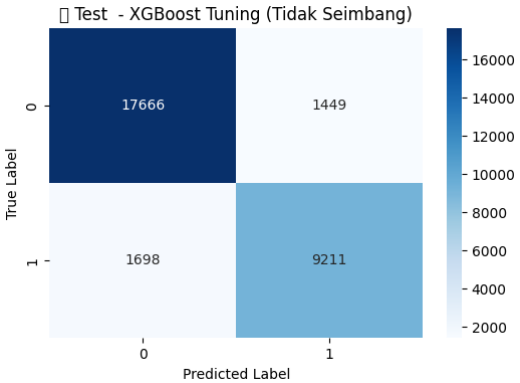
Evaluasi.	Train	Test
Accuracy	0.9111	0.9033
Precision	0.9115	0.9036
Recall	0.9111	0.9033
F1-Score	0.9111	0.9033

c. Model Tuning Hyperparameter data tidak seimbang
Model ketiga menerapkan tuning hyperparameter dengan Random Search namun masih menggunakan data tidak seimbang. Tujuan skenario ini adalah melihat seberapa besar pengaruh tuning terhadap data yang belum diperbaiki. Dimana Gambar 9 menunjukkan sedikit peningkatan, dengan akurasi pada data uji naik menjadi 0.8952, dan metrik lainnya mengalami perbaikan kecil.



Gambar 9. Train - XGBoost Tuning (Tidak Seimbang)

Gambar 10 memperlihatkan hasil pengujian terhadap mode yang sudah dituning, tetapi masih menggunakan data tidak seimbang, hasilnya menunjukan adanya peningkatan dibandingkan model awal.



Gambar 10. Test - XGBoost Tuning (Tidak Seimbang)

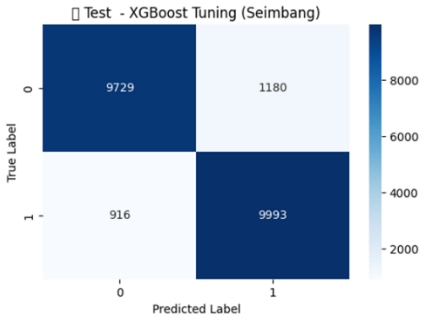
Berikut adalah tabel 4 yaitu tabel metrik evaluasi untuk melihat perbandingan performa model sebelum dan sesudah dilakukan tuning hyperparameter pada data tidak seimbang :

Tabel 4. Tuning Hyperparameter data tidak seimbang

Evaluasi.	Train	Test
Accuracy	0.9061	0.8952
Precision	0.9058	0.8948
Recall	0.9061	0.8952
F1-Score	0.9059	0.8949

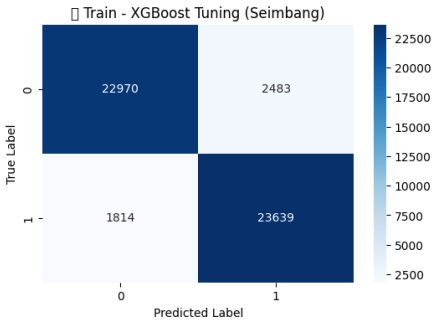
d. Model XGBoost dengan Tuning Hyperparameter Random Search dengan data Seimbang
Model keempat adalah gabungan dari dua pendekatan terbaik: data yang telah diseimbangkan dan tuning hyperparameter. Seperti pada Gambar 11, model ini menunjukkan hasil tertinggi secara keseluruhan, dengan akurasi uji 0.9039 dan precision 0.9042, menjadikannya model terbaik di antara semua skenario.

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920



Gambar 11. Train - XGBoost Tuning (Seimbang)

Gambar 12 menunjukkan hasil pengujian akhir dari model terbaik yang telah dituning dan menggunakan data seimbang, model ini berhasil memberikan prediksi yang paling akurat dan seimbang.



Gambar 12. Test - XGBoost Tuning (Seimbang)

Untuk melihat sejauh mana peningkatan performa, berikut disajikan tabel 5 yang merupakan tabel evaluasi lengkap yang mencakup nilai accuracy, precision, recall, dan F1-score dari hasil klasifikasi.

Tabel 5. Model Tuning Hyperparameter data seimbang

Evaluasi.	Train	Test
Accuracy	0.9156	0.9039
Precision	0.9159	0.9042
Recall	0.9156	0.9039
F1-Score	0.9156	0.9039

Berdasarkan hasil evaluasi dari keempat model, dapat disimpulkan bahwa Model XGBoost dengan Tuning Hyperparameter menggunakan Random Search dan data yang telah diseimbangkan (Tabel 5) menunjukkan kinerja terbaik dibandingkan model-model lainnya. Hal ini terlihat dari nilai akurasi tertinggi pada data pengujian sebesar 0.9039, yang sedikit lebih tinggi dibandingkan model tanpa tuning atau tanpa penyeimbangan data.

4. KESIMPULAN

Penelitian ini dilakukan untuk mengevaluasi performa algoritma Extreme Gradient Boosting (XGBoost) dalam mengklasifikasikan website phishing, dengan fokus pada dua pendekatan utama: penanganan data tidak seimbang menggunakan Radial Based Undersampling (RBU) dan tuning hyperparameter menggunakan metode Random Search. Berdasarkan serangkaian eksperimen yang dilakukan, diperoleh beberapa kesimpulan sebagai berikut. Model XGBoost tanpa penyeimbangan data menunjukkan akurasi sebesar 0.9019 pada data latih dan 0.8947 pada data uji. Metrik precision, recall, dan F1-score pada kedua data tersebut juga menunjukkan nilai yang relatif seimbang, namun performa model masih belum optimal dalam menangani ketimpangan distribusi kelas, khususnya dalam mengenali kelas minoritas. Model XGBoost dengan penyeimbangan data menggunakan RBU memberikan peningkatan performa, dengan akurasi sebesar 0.9111 pada data latih dan 0.9033 pada data uji. Nilai precision, recall, dan F1-score yang lebih tinggi menunjukkan bahwa penggunaan RBU berhasil meningkatkan kemampuan model dalam mengenali kelas minoritas, sehingga performa model menjadi lebih adil dan seimbang. Hal ini membuktikan bahwa metode Radial Based Undersampling berhasil menyeimbangkan distribusi data antar kelas, sehingga model dapat melakukan klasifikasi secara lebih optimal dan tidak bias terhadap kelas mayoritas. Model XGBoost dengan tuning hyperparameter tanpa penyeimbangan data menghasilkan akurasi sebesar 0.9061 pada data latih dan 0.8952 pada data uji. Tuning hyperparameter menggunakan Random Search terbukti mampu meningkatkan kemampuan generalisasi model, meskipun data tetap dalam kondisi tidak seimbang. Model XGBoost dengan tuning hyperparameter pada data seimbang (RBU) menunjukkan performa terbaik secara keseluruhan, dengan akurasi sebesar 0.9156 pada data latih

Building of Informatics, Technology and Science (BITS)
Volume 7, No 2, September 2025 Page: 1153−1163
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v7i2.7920

dan 0.9039 pada data uji. Metrik evaluasi lainnya seperti precision, recall, dan F1-score juga menunjukkan hasil yang optimal dan seimbang. Hal ini menunjukkan bahwa kombinasi teknik penyeimbangan data dan tuning hyperparameter merupakan strategi paling efektif dalam membangun model klasifikasi phishing yang akurat dan adil.

REFERENCES

[1] V. A. Windarni, A. F. Nugraha, S. T. A. Ramadhani, D. A. Istiqomah, F. M. Puri, and A. Setiawan, "Deteksi Website Phishing Menggunakan Teknik Filter Pada Model Machine Learning," *Inf. Syst. J.*, vol. 6, no. 01, pp. 39–43, 2023, doi: 10.24076/infosjournal.2023v6i01.1268.

[2] A. Raihan, M. Fadhli, T. Engineering, and P. N. Sriwijaya, "Implementation Of Deep Learning For Detecting Phishing Attacks On Websites With Combination Of Cnn And Lstm Implementasi Deep Learning Dalam Mendeteksi Serangan," *J. Tek. Inform.*, vol. 5, no. 5, pp. 1451–1459, 2024, doi: 10.52436/1.jutif.2024.5.5.2446.

[3] T. F. Handoyo, M. Pajar, and K. Putra, "Optimasi Bobot Kelas LSTM untuk Deteksi URL Phishing pada Dataset Tidak Berimbang," *J. Inform. J. Pengemb. IT*, vol. 10, no. 1, pp. 20–36, 2025, doi: 10.30591/jpit.v10i1.8128.

[4] M. Erkamim, S. Suswadi, M. Z. Subarkah, and E. Widarti, "Komparasi Algoritme Random Forest dan XGBoosting dalam Klasifikasi Performa UMKM," *J. Sist. Inf. Bisnis*, vol. 13, no. 2, pp. 127–134, 2023, doi: 10.21456/vol13iss2pp127-134.

[5] M. W. Dwinanda, N. Satyahadewi, and W. Andani, "Classification of Student Graduation Status Using Xgboost Algorithm," *BAREKENG J. Ilmu Mat. dan Terap.*, vol. 17, no. 3, pp. 1785–1794, 2023, doi: 10.30598/barekengvol17iss3pp1785-1794.

[6] L. Wulandari, "Optimisasi Algoritma Xgboost Untuk Prediksi Hasil Pemilu," *J. Dunia Data*, vol. 1, no. 5, pp. 1–16, 2024, [Online]. Available: http://www.portaldata.org/index.php/duniadata/article/view/100

[7] A. Syukron, S. Sardiarinto, E. Saputro, and P. Widodo, "Penerapan Metode Smote Untuk Mengatasi Ketidakseimbangan Kelas Pada Prediksi Gagal Jantung," *J. Teknol. Inf. dan Terap.*, vol. 10, no. 1, pp. 47–50, 2023, doi: 10.25047/jtit.v10i1.313.

[8] M. Kavitha, "Comparative Analysis of SMOTE Techniques and Machine Learning Models for Imbalanced Medical Datasets," *IEEE Conf. Proc.*, June, 2024

[9] K. Omari and A. Oukhatar, "Advanced Phishing Website Detection with SMOTETomek-XGB: Addressing Class Imbalance for Optimal Results," *Procedia Comput. Sci.*, vol. 252, pp. 289–295, 2025, doi: 10.1016/j.procs.2024.12.031.

[10] M. Adhikari and S. Pandey, "A Comparative Analysis of Support Vector Machines , Decision Trees , and Long Short-Term Memory Networks in Phishing Website Detection," *Int. J. Res. Publ.*, vol. 159, no. 1, pp. 190–199, 2024, doi: 10.47119/IJRP100159110202472261.

[11] A. Kharis Pratama, H. Ashaury, and F. Rakhmat Umbara, "Klasifikasi Data Gempa Bumi Di Pulau Jawa Menggunakan Algoritma Extreme Gradient Boosting," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 4, pp. 2923–2929, 2024, doi: 10.36040/jati.v7i4.7296.

[12] D. Kurnia, M. Itqan Mazdadi, D. Kartini, R. Adi Nugroho, and F. Abadi, "Seleksi Fitur dengan Particle Swarm Optimization pada Klasifikasi Penyakit Parkinson Menggunakan XGBoost," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 5, pp. 1083–1094, 2023, doi: 10.25126/jtiik.20231057252.

[13] M. Koziarski, "Radial-Based Undersampling Algorithm for Classification of Breast Cancer Histopathological Images Affected by Data Imbalance," *Pattern Recognit.*, no. 1, pp. 2–6, 2019, doi: 10.1016/j.patcog.2020.107262.

[14] M. Dava Maulana, A. Id Hadiana, and F. Rakhmat Umbara, "Algoritma Xgboost Untuk Klasifikasi Kualitas Air Minum," *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 7, no. 5, pp. 3251–3256, 2024, doi: 10.36040/jati.v7i5.7308.

[15] A. C. Nugraha and M. I. Irawan, "Komparasi Deteksi Kecurangan pada Data Klaim Asuransi Pelayanan Kesehatan Menggunakan Metode Support Vector Machine (SVM) dan Extreme Gradient Boosting (XGBoost)," *J. Sains dan Seni ITS*, vol. 12, no. 1, 2023, doi: 10.12962/j23373520.v12i1.107032.

[16] L. Zhang, W. Bian, W. Qu, L. Tuo, and Y. Wang, "Time series forecast of sales volume based on XGBoost," *J. Phys. Conf. Ser.*, vol. 1873, no. 1, 2021, doi: 10.1088/1742-6596/1873/1/012067.

[17] Y. Rombe, S. A. Thamrin, and A. Lawi, "Application of Adaptive Synthetic Nominal and Extreme Gradient Boosting Methods in Determining Factors Affecting Obesity: A Case Study of Indonesian Basic Health Research Survey 2013," *Indones. J. Stat. Its Appl.*, vol. 6, no. 2, pp. 309–317, 2022, doi: 10.29244/ijsa.v6i2p309-317.

[18] S. Fatika, N. Halim, and D. Aktuaria, "Analisis Perbandingan Klasifikasi dan Penerapan SMOTE Dalam Imbalanced Data pada Credit Card Default," *J. Sains dan Seni ITS 12(2)*, vol. 12, no. 2, 2023, doi: 10.12962/j23373520.v12i2.111833.

[19] M. Fajri and A. Primajaya, "Komparasi Teknik Hyperparameter Optimization pada SVM untuk Permasalahan Klasifikasi dengan Menggunakan Grid Search dan Random Search," *J. Appl. Informatics Comput.*, vol. 7, no. 1, pp. 14–19, 2023, doi: 10.30871/jaic.v7i1.5004.

[20] Euis Saraswati, Yuyun Umaidah, and Apriade Voutama, "Penerapan Algoritma Artificial Neural Network untuk Klasifikasi Opini Publik Terhadap Covid-19," *Gener. J.*, vol. 5, no. 2, pp. 109–118, 2021, doi: 10.29407/gj.v5i2.16125.

[21] L. M. Sausan, Desty Mayang Pratiwi, "Perbandingan Metode Decision Tree Classifier dan XGBoost Classifier Dalam Memprediksi Penyakit Jantung," *CENTIVE*, vol. 4, pp. 991–1000, 2024, [Online]. Available: https://conferences.ittelkom-pwt.ac.id/index.php/centive/article/download/336/303

[22] I. U. W. Mulyono, E. H. Rachmawanto, C. A. Sari, and M. K. Sarker, "A high accuracy of deep learning based CNN architecture: classic, VGGNet, and RestNet50 for Covid-19 image classification," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 22, no. 5, pp. 1187–1195, 2024, doi: 10.12928/TELKOMNIKA.v22i5.26017.