

# Implementasi Algoritma J48 Untuk Identifikasi Website Phising

Ryan Putra Ramadhan<sup>1</sup>, Teti Desyani<sup>2\*</sup>

<sup>1,2</sup>Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia

Email: <sup>1</sup>[rayenp09@gmail.com](mailto:rayenp09@gmail.com), <sup>2\*</sup>[dosen00839@unpam.ac.id](mailto:dosen00839@unpam.ac.id)

**Abstrak** – Implementasi algoritma J48 pada identifikasi website phishing merupakan suatu teknik yg dipergunakan buat memprediksi apakah suatu website termasuk pada kategori phishing atau tidak. algoritma J48 adalah salah satu jenis prosedur pemecahan Decision Tree yg populer dipergunakan pada bidang pengolahan data dan pembelajaran mesin pada aplikasi weka. di implementasi ini, link domain website yang akan diidentifikasi dianalisis. Proses identifikasi website phishing menggunakan prosedur pemecahan J48 ini bisa menaikkan efektivitas serta efisiensi untuk mendeteksi website phishing. karena, prosedur pemecahan J48 bisa membentuk contoh yang mudah dipahami serta digunakan sang mesin mengklasifikasikan website. tetapi demikian, pada implementasi algoritma J48, diharapkan data yang berkualitas dan bervariasi buat mendapatkan akibat yang optimal. Selain itu, penggunaan algoritma ini pula tidak sepenuhnya menjamin 100% keakuratan pada mendeteksi website phishing, menjadi akibatnya perlu dilakukan evaluasi, fitur fitur tambahan yg dapat memprediksi suatu situs secara akurat serta diperlukannya kombinasi algoritma yang lainnya.

**Kata Kunci:** Algoritma J48, Phising, Website, Decision Tree, Klasifikasi

**Abstract** – The implementation of the J48 algorithm in phishing website identification is a technique used to predict whether a website falls into the category of phishing or not. The J48 algorithm is one type of Decision Tree solving procedure that is popularly used in the field of data processing and machine learning in the Weka application. In this implementation, the domain link of the website to be identified is analyzed. The phishing website identification process using the J48 solving procedure can increase the effectiveness and efficiency of detecting phishing websites. This is because the J48 solving procedure can form easily understood examples and be used by machines to classify websites. However, in the implementation of the J48 algorithm, high-quality and varied data is required to achieve optimal results. Additionally, the use of this algorithm does not guarantee 100% accuracy in detecting phishing websites, so evaluation and additional features that can accurately predict a site are needed, as well as the need for the combination of other algorithms.

**Keywords:** Algoritma J48, Phising, Website, Decision Tree, Klasifikasi

## 1. PENDAHULUAN

Jumlah pengguna internet di Indonesia meningkat menjadi 196,7 juta jiwa hingga kuartal II 2020. Jika pada 2018 lalu, jumlah pengguna internet di Indonesia hanya sebesar 171,2 juta jiwa. Hal tersebut diketahui berdasarkan hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Survei tersebut dilakukan pada 2 sampai 25 Juni 2020 menurut (Akhdhi Martin Pratama, 2020).

Saat ini internet sudah menjadi bagian penting dalam kehidupan masyarakat terutama pada aktifitas sosial dan finansial. Sebagai contohnya media sosial yang digunakan sebagai sarana berkomunikasi, mencari teman dan juga bisnis online yang digunakan beberapa pihak terutama perusahaan untuk menawarkan perdagangan online melalui e-mail dan memberitahu kepada calon pelanggan tentang website mereka, namun saat ini ada pihak yang tidak bertanggung jawab melakukan tindakan yang merugikan banyak orang yang salah satunya adalah tindakan *phising*.

Situs *phising* merupakan sebuah website yang didesain oleh penjahat internet sedemikian rupanya agar menyerupai situs otentik (tampilan, konten, URL domain atau lainnya) untuk mengelabui korbannya (pengguna internet) dengan membuat korban seolah-olah sedang mengakses halaman situs dari sumber yang sah. Tampilan situs akan dibuat semirip mungkin dengan situs aslinya agar korban yakin sedang berada pada situs yang benar.

Selain itu, ada pula situs *phising* yang didesain khusus untuk memberikan informasi atau petunjuk palsu yang menyesatkan. Jika korban berhasil dikelabui dan memasukkan informasi yang diminta, penjahat internet dapat dengan mudah menggunakan informasi tersebut pada situs yang sah

untuk melakukan aktifitas-aktifitas yang tidak diinginkan dan tentunya hal ini akan menimbulkan kerugian yang cukup signifikan bagi para korbannya mulai dari kerugian finansial hingga data loss.

Sebanyak 1353 situs web dengan 10 variabel telah dikumpulkan didalam data tersebut. situs web palsu dikumpulkan dari arsip data Phishtank yang merupakan situs komunitas gratis tempat pengguna dapat mengirimkan, memverifikasi, melacak dan berbagi data phishing. Situs web yang sah dikumpulkan dari yahoo dan direktori titik awal menggunakan skrip web yang dikembangkan dalam PHP. Skrip PHP dicolokkan dengan browser dan telah mengumpulkan 548 situs web resmi dari 1353 situs web. ada 702 URL phishing, dan 103 URL mencurigakan (Abdelhamid, 2016)

Menurut APWG (Anti-Phishing Working Group), kesadaran masyarakat terhadap situs *phishing* meningkat dari tahun ke tahun, akan tetapi jumlah situs *phishing* dan kerugian yang ditimbulkan tumbuh lebih cepat. Pada laporan APWG kuartal keempat 2016, pada bulan Oktober 2016 terdapat 89,232 situs yang terdeteksi sebagai situs *phishing*, sedangkan di bulan November dan Desember 2016 masing-masing terdapat 118.928 dan 69.533 situs yang terindikasi sebagai situs *phishing*. Pada laporan tersebut juga ditemukan kurang lebih 17 juta malware baru, Hal ini dapat menimbulkan ketakutan dan menurunnya kepercayaan pengguna internet bertransaksi secara online, padahal transaksi secara online saat ini sedang booming di Indonesia.

Menurut laporan dari Kaspersky Security Network pada tahun 2021, serangan phishing menjadi ancaman keamanan siber nomor satu di Indonesia, dengan sekitar 1,6 juta serangan phishing terdeteksi selama periode kuartal keempat 2020. Serangan phishing juga merupakan ancaman terbesar di Asia Tenggara secara keseluruhan, dengan Indonesia menempati posisi teratas dalam hal jumlah serangan phishing. Beberapa faktor yang menyebabkan peningkatan serangan *phishing* di Indonesia antara lain semakin banyaknya pengguna internet di Indonesia, kurangnya kesadaran akan keamanan siber, dan kelemahan dalam keamanan infrastruktur internet. Selain itu, banyaknya pengguna internet yang masih belum teredukasi dengan baik mengenai taktik dan strategi yang digunakan oleh pelaku *phishing* juga menjadi faktor penyebab.

Upaya pencegahan dan penanganan serangan *phishing* juga semakin penting di Indonesia. Beberapa langkah yang dapat dilakukan untuk mencegah serangan *phishing* di antaranya adalah meningkatkan kesadaran dan edukasi tentang keamanan siber, menggunakan teknologi keamanan seperti proteksi dari malware, keamanan jaringan, dan penggunaan sertifikat SSL pada situs web, serta menindak tegas pelaku kejahatan dunia maya yang melakukan serangan *phishing*. Selain itu, peran aktif dari lembaga pemerintah dan penegak hukum juga sangat penting dalam penanganan serangan *phishing* di Indonesia.

Beberapa lembaga pemerintah seperti Kementerian Komunikasi dan Informatika (Kemenkominfo) dan Badan Siber dan Sandi Negara (BSSN) telah melakukan upaya-upaya dalam meningkatkan kesadaran dan edukasi mengenai keamanan siber, serta melakukan pengawasan dan penindakan terhadap kasus-kasus serangan *phishing*. Dalam penelitian yang dilakukan oleh Amelia et al. (2020) yang berjudul "*Phishing Prevention Using Two Factor Authentication in Indonesia*", hasil penelitian menunjukkan bahwa penggunaan metode autentikasi dua faktor dapat membantu dalam mencegah serangan *phishing* di Indonesia. Metode autentikasi dua faktor ini dapat meningkatkan keamanan akun online dengan memerlukan pengguna untuk memasukkan kode verifikasi yang dikirimkan melalui SMS atau aplikasi otentikator selain memasukkan username dan password. Internet telah memberikan kemudahan bagi kita untuk mengakses informasi, melakukan transaksi bisnis, berkomunikasi dengan orang lain, dan banyak lagi. Namun, bersamaan dengan manfaat tersebut, ada pula risiko keamanan siber yang harus diwaspadai, salah satunya adalah *phishing*. Phishing adalah suatu praktik penipuan yang dilakukan dengan cara membuat situs web palsu yang meniru situs web asli dari suatu perusahaan atau organisasi terkenal, seperti bank atau situs web e-commerce, dengan tujuan memperoleh informasi pribadi dari pengguna seperti nama pengguna, kata sandi, atau nomor kartu kredit.

Terlebih lagi masih banyak masyarakat Indonesia yang masih suka mengshare website *phishing* khususnya di whatsapp grub menjadikannya awal mula pembuatan penelitian ini, karna hal ini dibutuhkan sebuah sistem yang mampu mendeteksi website *phishing* untuk mencegah terjadinya kerugian yang ditimbulkan oleh website *phishing* kepada pengguna internet.

Dikarenakan masih minimnya penelitian ini dan beberapa penelitian sebelumnya memfokuskan pada nilai confusion matrix untuk memperoleh hasil akurasi, nilai precision, nilai recall dan nilai f-measure pada algoritma yang digunakan pada penelitian ini, peneliti juga akan melakukan pendekatan berbasis URL untuk membuat sebuah sistem model klasifikasi deteksi situs *phising*.

## 2. METODOLOGI PENELITIAN

Metodologi penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Penggunaan metode dalam melakukan penelitian, bermanfaat untuk mendukung pembuatan laporan berdasarkan data yang diperoleh selama melakukan penelitian tersebut. Dalam penyusunan skripsi ini, penulis menggunakan beberapa metode penelitian yang digunakan, yaitu

### 2.1 Metode Pengumpulan Data

#### a. Metode Pengamatan Langsung (Observasi)

Metode observasi akan digambarkan sebagai metode yang dipergunakan dalam mengamati dan mendeskripsikan tingkah laku subjek. Seperti namanya, observasi ini adalah cara mengumpulkan informasi dan data yang relevan dengan mengamati. Pada penelitian ini, peneliti juga akan melakukan pendekatan berbasis URL untuk membuat model klasifikasi deteksi situs *phising* di Indonesia.

#### b. Metode Literatur (Library Research)

Dalam hal ini untuk mengumpulkan data dan cara mencari referensi teori yang relevan dengan kasus atau permasalahan yang ditemukan. Referensi ini didapat dari jurnal, artikel laporan penelitian, dan situs-situs di internet, yang ada kaitannya dengan penelitian ini

#### c. Dokumentasi

Berupa file file, foto, rekaman dll

### 2.2 Metode Pengembangan Sistem

Metodologi pengembangan perangkat lunak atau metodologi pengembangan sistem adalah suatu kerangka kerja yang digunakan untuk menstrukturkan, merencanakan, dan mengendalikan proses pengembangan suatu sistem informasi. Metodologi yang digunakan dalam perancangan implementasi algoritma j48 untuk menentukan website *phising* adalah waterfall. Aktifitas-aktifitas dalam metodologi waterfall adalah :

#### a. Analisä

Merupakan tahap menganalisis hal-hal yang diperlukan dalam pelaksanaan pembangunan sistem penilaian kompetensi.

#### b. Design

Tahap penerjemahan dari data yang di analisis kedalam bentuk yang mudah dan dimengerti dan diinginkan oleh user. Desain dalam bentuk usecase, activity diagram, desain basis data, dan desain antar muka sistem.

#### c. Coding

Tahap penerjemahan dari data atau pemecahan masalah yang telah didesain kedalam Bahasa pemrograman. Yaitu proses pembangunan sistem identifikasi website *phising* yang akan dibangun dalam bentuk web.

#### d. Testing

Merupakan tahap pengujian perangkat lunak yang akan dibangun

### 2.3 Algoritma J48

Algoritma yang merupakan pengembangan dari ID3 ini dapat mengklasifikasikan data dengan metode pohon keputusan yang memiliki kelebihan dapat mengolah data numerik (kontinyu) dan diskret, dapat menangani nilai atribut yang hilang, menghasilkan aturan-aturan yang mudah diinterpretasikan, dan tercepat diantara algoritma-algoritma yang menggunakan memori utama di komputer.

Pada penerapan beberapa kasus teknik klasifikasi, algoritma ini mampu menghasilkan performansi yang bagus. Dengan kelebihan inilah diharapkan algoritma ini bisa menangani studi kasus secara optimal dan diharapkan juga tentunya bagi algoritma ini untuk menghasilkan akurasi dan performansi yang baik.

Algoritma J48 merupakan implementasi dari algoritma C4.5 di dalam aplikasi WEKA. Algoritma ini menghasilkan pohon keputusan yang dapat digunakan untuk mengklasifikasikan suatu data ke dalam kelas-kelas dan juga memprediksi kelas dari suatu data (Agustiani, 2020).

Terdapat empat langkah dalam proses pembuatan pohon keputusan pada algoritma C4.5, yaitu:

- Memilih atribut sebagai akar, didasarkan pada nilai gain tertinggi dari atribut-atribut yang ada.
- Membuat cabang untuk masing-masing nilai, artinya membuat cabang sesuai dengan jumlah nilai variabel gain tertinggi.
- Membagi setiap kasus dalam cabang, berdasarkan perhitungan nilai gain tertinggi dan perhitungan dilakukan setelah perhitungan nilai gain tertinggi awal dan kemudian dilakukan proses perhitungan gain tertinggi kembali tanpa meyertakan nilai variabel gain awal.
- Mengulangi proses dalam setiap cabang sehingga semua kasus dalam cabang memiliki kelas yang sama, mengulangi semua proses perhitungan gain tertinggi untuk masing-masing cabang kasus sampai tidak bisa lagi dilakukan proses perhitungan.

## 3. ANALISA DAN PEMBAHASAN

Analisis data digunakan untuk mengolah data menjadi informasi, data akan menjadi lebih mudah dipahami dan diinterpretasikan data yang di analisa adalah data yang telah di ambil dari internet yang bersumber dari <https://www.kaggle.com/> hasilnya peneliti memperoleh 50 dataset website di bawah ini adalah data yang peneliti dapat.

**Tabel 1.** Tabel Data *Phising*

No	Penggunaan slash	Penggunaan https	Penggunaan IP	Jumlah DOT (.)	Panjang URL	PENGUNAAN AT "@"	Hasil
1	1	1	0	0	1	1	yes
2	1	0	0	1	0	1	yes
3	1	1	0	1	1	0	no
4	1	0	0	1	1	1	no
5	1	1	0	0	1	0	no
6	1	0	1	1	1	1	no
7	1	0	1	1	0	1	yes
8	1	0	1	1	1	1	yes
9	1	0	1	1	1	1	yes
10	1	0	0	0	1	0	yes
11	0	0	1	1	0	1	yes
12	0	1	0	1	0	0	yes

13	0	1	1	0	0	1	yes
14	0	1	1	1	0	1	yes
15	0	1	1	1	1	0	yes
16	0	1	1	1	0	1	no
17	1	1	0	0	0	1	no
18	1	1	0	0	0	0	no
19	0	1	0	1	0	1	no
20	1	1	0	0	0	1	no
21	1	1	0	0	0	1	no
22	0	1	1	0	1	0	no
23	1	1	1	0	1	1	no
24	0	1	1	0	1	1	no
25	1	1	0	0	1	0	yes
26	0	1	0	1	1	1	no
27	1	1	1	1	1	1	no
28	1	0	0	0	0	1	yes
29	1	0	1	0	1	0	no
30	1	0	0	1	1	1	no
31	1	0	1	1	0	0	no
32	1	0	1	1	1	0	no
33	1	0	1	1	0	1	yes
34	0	0	1	0	0	0	yes
35	0	1	0	1	0	1	yes
36	0	0	0	1	1	0	yes
37	0	0	1	1	1	0	yes
38	0	0	0	0	1	0	yes
39	0	1	0	1	1	1	yes
40	1	0	0	0	1	1	yes
41	1	1	1	1	0	0	yes
42	1	0	1	0	0	1	no
43	1	1	1	0	0	1	no
44	0	1	1	1	1	0	no
45	1	1	0	0	0	0	no
46	1	1	0	0	1	0	no
47	1	0	0	0	1	0	no
48	1	0	1	1	0	0	yes
49	1	1	1	0	1	0	no
50	1	1	0	0	1	0	no

Dari data di atas dihitung menggunakan rumus algoritma J48 yang merupakan implementasi algoritma C4.5 pada weka, Algoritma C4.5 dapat menangani data numerik (kontinyu) dan diskret,

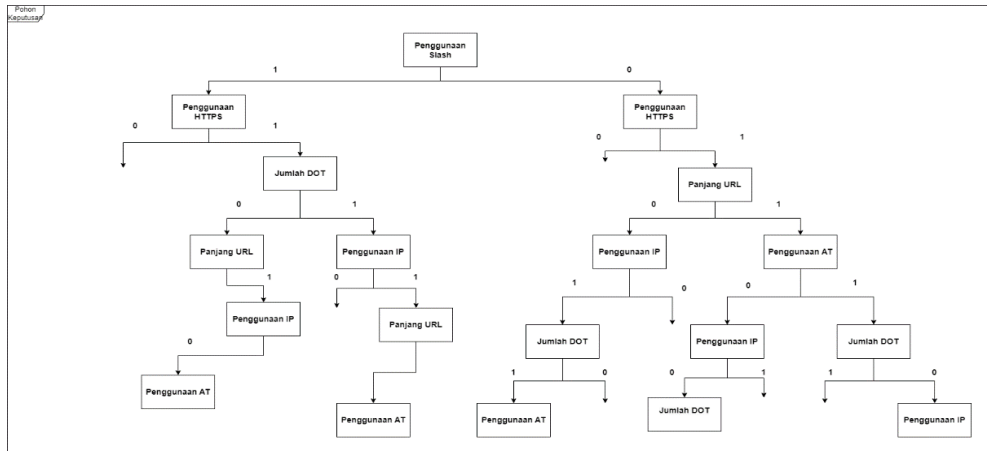
dalam algoritma C4.5 digunakan information gain untuk memilih atribut yang akan digunakan untuk pemisah obyek. Pemilihan atribut akan menempati simpul dengan melakukan perhitungan entropi dan mencari nilai paling minimum, Proses C4.5, dengan memilih atribut sebagai akar (root), buat cabang untuk tiap nilai, bagi kasus ke dalam cabang, ulangi proses untuk tiap cabang hingga semua cabang memiliki kelas yang sama. Atribut akar dipilih berdasar nilai gain tertinggi yang membutuhkan nilai perhitungan entropy. Entropy adalah ukuran dari teori informasi yang dapat mengetahui karakteristik dari impurity, dan homogeneity dari kumpulan data. Entropy mengukur jumlah dari informasi yang ada pada atribut. Analisa dalam penelitian algoritma J48 ini akan menggunakan pohon keputusan berdasarkan penentuan atribut yang digunakan kemudian menghitung entropy total dan gain total dari setiap atributnya, kemudian menuliskan proses perhitungan entropy dan gain total, selanjutnya mengeksekusi semua atribut yang akan digunakan, selanjutnya menghasilkan pohon keputusan dan proses selesai.

**Tabel 2.** Pencarian Gain Tertinggi

	Nilai	Jumlah	Yes	No	Entrhopy	Gains
Total		50	23	27	0,995378	
<b>HTTPS</b>				0		0,052776
	1	33	12	21	0,94566	
	0	17	11	6	0,936667	
<b>Penggunaan Slash</b>						0,071968
	1	28	9	19	0,905928	
	0	22	14	8	0,94566	
<b>Penggunaan IP</b>						0,001162
	1	25	12	13	0,998846	
	0	25	11	14	0,989588	
<b>Jumlah Dot</b>						0,04351
	1	26	15	11	0,982859	
	0	24	8	16	0,918296	
<b>Panjang URL</b>						0,016699
	1	28	11	17	0,966619	
	0	22	12	10	0,99403	
<b>Penggunaan AT</b>						0,001574
	1	27	13	14	0,99901	
	0	23	10	13	0,987693	

Maka dari hasil perhitungan algoritma di atas dapat disimpulkan bahwa nilai penggunaan slash menjad nilai gain terbesar Hasil perhitungan yang tertera pada masing tabel diatas didapatkan nilai gain tertinggi pada atribut penggunaan slash dengan nilai gain 0.072, Selanjutnya atribut terpilih (atribut dengan nilai gain tertinggi) yaitu penggunaan slash akan menjadi node akar untuk membangun decision tree, proses perhitungan entropy dan gain akan terus berulang jika masih ada record yang masih terpartisi (masih membentuk node baru) dan akan berhenti jika semua record sudah memiliki keputusan. Untuk perhitungan entropy dan gain pada proses selanjutnya (node cabang) rumusnya sama dengan rumus mencari node akar hanya saja pada proses node baru tidak menyertakan atribut yang sudah menjadi node akar atau atribut yang sudah memiliki keputusan, Pada gambar berikut adalah hasil decision tree akhir dimana semua record sudah terpartisi dan telah

memiliki aturan keputusan, Adapun pohon keputusan yang telah di dapatkan dari perhitungan pada tabel di atas adalah :



**Gambar 1** Hasil Pohon Keputusan

### 3.1 Sistem yang diusulkan

Pada tahap ini, penulis ingin membuat sistem baru untuk identifikasi website *phising* yang dimana ketika user menginputkan alamat website maka akan secara otomatis mengidentifikasi sesuai dengan fitur fitur yang ada sebagai bahan penilaian untuk mendapatkan hasil.

Penelitian ini akan menghasilkan suatu aplikasi web yang digunakan untuk identifikasi website *phising* maka dibutuhkannya suatu input dan output sistem agar aplikasi dapat berjalan dengan lancar.

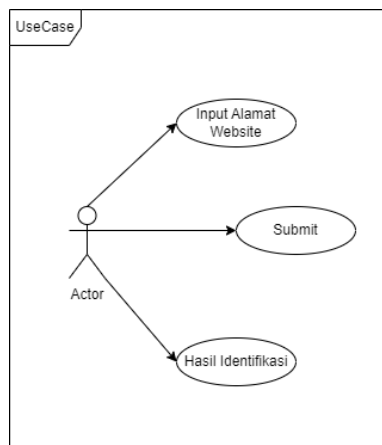
a. Input Sistem

Input alamat web yang ingin di identifikasi

b. Output Sistem

Informasi terkait hasil identifikasi

Use case diagram merupakan pemodelan untuk menggambarkan kelakuan dari sistem yang dibuat dan mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang dibuat serta digunakan untuk mengetahui fungsi apa saja yang ada didalam sebuah sistem dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut. Pada gambar 2 digambarkan mengenai *use case* diagram dari sistem yang dibuat dimana terdapat aktor yaitu pengguna. Aktor pengguna memiliki hak untuk mengidentifikasi website itu *phising* atau tidak.



**Gambar 2.** Usecase Diagram

## 4. IMPLEMENTASI

Pada bab ini akan dipaparkan implementasi sistem berdasarkan rancangan program. rancangan sistem yang telah di bangun akan implementasikan ke dalam bentuk *sourcecode* dalam bahasa pemrograman web.

### 4.1 Implementasi Aplikasi

Hasil penelitian ini merupakan tahap akhir dalam mewujudkan hasil rancangan menjadi sebuah sistem. Yang dimana sistem dapat berjalan pada komputer sedang online, jika ingin menjalankannya secara online maka harus di hosting terlebih dahulu. Penelitian ini mengimplementasikan sistem ini dengan hosting supaya dapat diakses dimana saja dan kapan saja selama terkoneksi internet.

Langkah – langkah menjalankan sistem ini adalah dengan mengakses alamat <https://e-phising.000webhostapp.com/> pada browser dengan menggunakan alamat ini pengguna akan melihat tampilan awal situs. Lalu pengguna dapat menggunakan sitem ini yang telah tersedia.

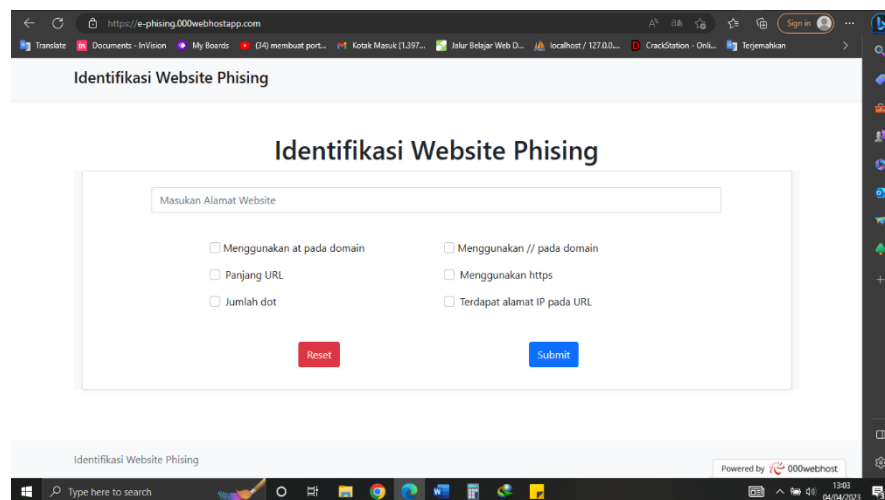
### 4.2 Implementasi Perangkat Lunak

Software yang digunakan untuk menjalankan Identifikasi Website *Phising* adalah sebagai berikut

**Tabel 3.** Tabel Spesifikasi Software

Nama	Spesifikasi
Sistem Operasi	Windows 10 Pro 64 bit
Browser	Google Chrome Version 111.0.5563.65 (Official Build) (64-bit)
Web Server	Xampp V 3.3.0
Code Editor	Sublime Text

### 4.3 Tampilan Antar Muka *Interface*



**Gambar 3.** Tampilan *Interface*

Pada gambar ini adalah gambar awal sebelum proses identifikasi pengguna harus mengisi kolom inputan dengan alamat website lalu klik tombol submit untuk proses identifikasi. Pada saat tombol submit di tekan maka 6 fitur yang terdapat di aplikasi maka akan otomatis tercentang apabila di alamat website yang di inputkan terdapat https pada domain, panjang url domain lebih dari 20 karakter, jumlah dot lebih atau sama dengan 3 pada domain, terdapat slash “/” pada domain, terdapat at “@” pada domain, terdapat IP pada domain, tombol reset akan menghapus inputan yang ada pada kolom inputan



## 5. KESIMPULAN

Aplikasi identifikasi web *phising* ini telah selesai dibuat setelah melakukan penelitian, riset data, membuat desain, lalu mengimplementasikannya dari design ke dalam bentuk sistem lalu mengujinya setelah sistem selesai di buat Maka dapat diperoleh beberapa kesimpulan sebagai berikut.

- a. Aplikasi ini sudah membantu dalam klasifikasi website *phising* dengan fitur yang sudah ditentukan.
- b. Aplikasi ini juga sangat mudah di gunakan di mana saja karna sudah online.
- c. Untuk hasil dari deteksi klasifikasi secara keseluruhan bekerja dengan baik, peneliti menggunakan Analisa alamat website berbasis URL

## REFERENCES

- Abdulloh, R. (2015). Easy & Simple Web Programming Belajar pemrograman website secara efektif dan efisien. Jakarta: Elex Media.
- Agung Susilo Yuda Irawan, . N. (2021). Identifikasi Website Phishing dengan Perbandingan Algoritma Klasifikasi. Syntax: Jurnal Informatika, 57-67.
- Agus Fatkhurohman, e. p. (2019). Penerapan Algoritma Naïve Bayes Classifier Untuk . Jurnal Teknologi Informasi, 115-124.
- Buulolo, E. (2020). Data Mining Untuk Perguruan Tinggi. Deepublish.
- Dimpos A P Situmorang, G. L. (2020). JURIKOM (Jurnal Riset Komputer), 530-536.
- Enterprise, J. (2017). Otodidak MySql Untuk Pemula. Jakarta: PT ELEX MEDIA KOMPUTINDO.
- Kaunan, F. J. (2018). Penerapan Algoritma J48 Decision Tree Untuk Analisis. Cogito Smart Journal, 248-257.
- M.Kom, M. H. (t.thn.). Algoritma Data Mining: Analisis Data Dengan Komputer. bisakimia.
- Meriska Defriani, I. J. (2020). ALGORITMA J48 DAN LOGISTIC MODEL TREE UNTUK MEMPREDIKSI . Journal of Information Technology and Computer Science (INTECOMS), 129-140.
- Muhamad Alda, S. K. (2021). Rekayasa Perangkat Lunak Berorientasi Objek. Media Sains Indonesia.
- Nabila Bianca Putri, A. W. (2019). Analisis Komparasi Algoritma Klasifikasi Data Mining Dalam Klasifikasi Website Phishing. Komputika: Jurnal Sistem Komputer, 59 - 66.
- Nurfaizah, M. I. (2017). ALGORITMA DECISION TREE-J48, K-NEAREST, DAN. Seminar Nasional Teknologi Informasi, 12-18.
- Pakpahan, N. S. (2021). Implementasi Data Mining Menggunakan Algoritma J48 Dalam Menentukan . Journal of Computing and Informatics Research, 07-13.
- Prof. Dr. Sri Mulyani, A. C. (2017). Analisis dan Perancangan Sistem Informasi Manajemen Keuangan Daerah: Notasi Pemodelan Unified Modeling Language (UML). Abdi Sistematika.
- Pungkas Subarkah, A. N. (2021). IDENTIFIKASI WEBSITE PHISHING MENGGUNAKAN ALGORITMA. Jurnal Ilmiah Informatika, 127-136.
- PURWANTONO, F. E. (2017). MODEL KLASIFIKASI UNTUK DETEKSI SITUS *PHISING* DI INDONESIA.
- Sa`ad, M. I. (2020). Otodidak Web Programming: Membuat Website Edutainment. Elex Media Komputindo.
- Setiawan, D. (2017). Buku Sakti Pemrograman Web: HTML, CSS, PHP, MySQL & Javascript. Jakarta: Anak Hebat Indonesia.
- Sunaryono. (2017). PENELITIAN KOMPARASI ALGORITMA KLASIFIKASI DALAM MENENTUKAN WEBSITE PALSU. Teknikom, 1-12.
- Suprianto, D. (2008). Buku Pintar Pemograman PHP. Bandung: Oase Media.
- Tomy Salim, Y. C. (2017). DATA MINING IDENTIFIKASI WEBSITE *PHISING* MENGGUNAKAN . Jurnal TAM (Technology Acceptance Model), 130-135.
- Wajhillah, R. Y. (2017). Penerapan Algoritma C4.5 Untuk Prediksi Penggunaan Jenis Kontrasepsi Berbasis Web. Kumpulan Jurnal Ilmu Komputer (KLIK), 174-187.