DETEKSI *WEBSITE PHISHING* MENGGUNAKAN TEKNIK FILTER PADA MODEL *MACHINE LEARNING*

Vikky Aprelia Windarni [1)], Anggit Ferdita Nugraha [2)], Surya Tri Atmaja Ramadhani [3)], Dewi Anisa Istiqomah [4)] , Fiyas Mahananing Puri [5)] , Adi Setiawan [6)]

[1)] Teknologi Informasi, Universitas AMIKOM Yogyakarta
[2)] Teknik Komputer, Universitas AMIKOM Yogyakarta
[3)] Teknik Informatika, Universitas AMIKOM Yogyakarta
[4)] Manajemen Informatika, Universitas AMIKOM Yogyakarta
[5)] Sistem Informasi, Universitas AMIKOM Yogyakarta
[6)] Fakultas Sains dan Matematika, Universitas Kristen Satya Wacana
email: vikkyaprelia@amikom.ac.id [1)], anggitferdita@amikom.ac.id [2)], surya@amikom.ac.id [3)], dewianisaist@amikom.ac.id [4)], fiyas@amikom.ac.id [5)] , adi.setiawan@uksw.edu [6)]

Abstraksi

Phishing merupakan bentuk serangan pada dunia maya yang cukup popular, dimana pengguna dibuat untuk mengunjungi situs *web* yang tidak sah. Pengguna ditipu untuk mengungkapkan informasi pribadinya seperti *username, password,* informasi kartu kredit dan sebagainya. Maraknya *phishing* membuat kerugian dalam hal *privacy*, bahkan terjadi penyalahgunaan data yang menyebabkan kerugian finansial. Tujuan dari penelitian ini adalah peneliti ingin menggunakan *machine learning* dengan memanfaatkan fitur filter yang ada didalamnya yaitu *pearson correlation* dan menerapkan 3 metode *Naïve Bayes*, *Decision Tree* dan *Random Forest* untuk menentukan metode yang paling efektif dalam mendeteksi *web phishing*. Terdapat 4 alur penelitian yang digunakan oleh peneliti, yaitu (1) Tahap persiapan, (2) Metode yang digunakan, (3) Analisa, dan (4) Evaluasi. Dari hasil penelitian ini didapatkan bahwa penerapan metode *Naïve Bayes* memiliki nilai akurasi sebesar 60,4%, metode *Decision Tree* memiliki nilai akurasi 94,4% dan metode *Random Forest* memiliki akurasi sebesar 96,3%. Sehingga dapat disimpulkan bahwa metode yang paling efektif untuk mendeteksi *web phishing* adalah menggunakan *Random Forest* karena memiliki tingkat akurasi sebesar 96.3%. Pada penelitian selanjutnya dapat dilakukan pada kasus yang sama dengan menggunakan algoritma yang berbeda.

Kata Kunci* : *Decision Tree, Naïve Bayes, Random Forest, Website Phishing

Abstract

Phishing is a fairly popular form of cyber attack, in which users are tricked into visiting legitimate websites. Users are tricked into disclosing personal information such as usernames, passwords, credit card information and so on. The rise of phishing makes losses in terms of privacy, even damages data which causes financial losses. The purpose of this study is that researchers want to use machine learning by utilizing the filter features in it, namely Pearson correlation and applying 3 methods of naïve Bayes, decision tree and random forest to determine the most effective method for detecting phishing websites. There are 4 research paths used by researchers, namely (1) the preparation stage, (2) the method used, (3) analysis, and (4) evaluation. From the results of this study, it was found that the application of the naïve Bayes method had an accuracy value of 60.4%, the decision tree method had an accuracy value of 94.4% and the random forest method had an accuracy of 96.3%. So, it can be concluded that the most effective method for detecting phishing websites is using a random forest because it has an accuracy rate of 96.3%. In further research, it can be carried out in the same case using a different algorithm.

Keywords*: *Decision Tree, Naïve Bayes, Random Forest, Website Phishing

1. Pendahuluan

Di era teknologi yang semakin berkembang ini orang-orang tidak bisa lepas dari sebuah internet maupun gadget. Perkembangan internet sejalan dengan perkembangan perangkat lunak yang semakin canggih. Internet adalah sebuah media informasi yang berguna untuk mencari sebuah informasi yang *up to date* dan dapat diakses secara global, akan tetapi internet juga dapat digunakan oleh *cybercrime* untuk mencuri data-data pribadi pengguna dengan cara menggunakan *phishing*.

Phishing adalah sebuah aktivitas penipuan dengan menggunakan alamat elektronik palsu maupun

website palsu untuk mendapatkan informasi tentang data pribadi seperti informasi pribadi (nama, alamat, jenis kelamin, tanggal lahir), informasi akun (nama pengguna dan kata sandi) atau informasi keuangan (informasi kartu kredit dan akun) [1]. Seseorang yang melakukan phishing biasanya disebut dengan phiser, phiser akan mengirim *email* yang tampaknya berasal dari bank, layanan dari sebuah *website* atau *malware*. *Phishing website* adalah salah satu metode *phising* yang dilakukan *cybercrime* dengan cara membuat *website* tiruan yang mirip dengan *website* aslinya. *Website* yang sering menjadi sasaran *phising* adalah *website* yang berkaitan dengan *online banking*, karena potensi yang diambil lebih tinggi dibandingkan dengan *website* yang lainnya.

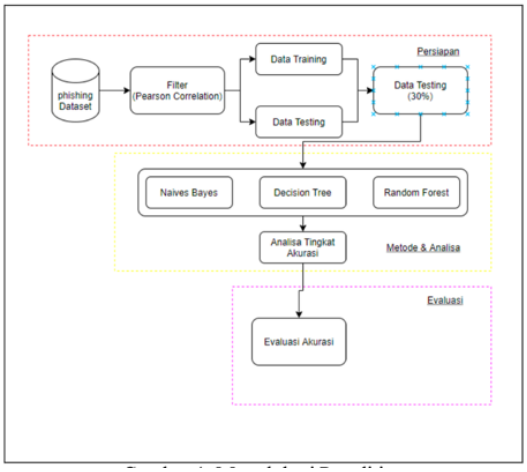
Machine Learning (ML) adalah suatu algoritma atau program komputer yang dapat membuat sistem menjadi cerdas dengan cara mempelajari data-data yang tersedia di mana algoritma atau program tersebut tidak didefinisikan secara eksplisit [2]. Implementasi *mechine learning* untuk dapat menyelesaikan permasalahan memiliki 3 syarat, yaitu membutuhkan memori yang besar dan dibutuhkan proses pelabelan dan tidak jarang hasil yang muncul tidak akurat. Bidang *machine learning* berkaitan dengan bagaimana membangun sebuah computer agar meningkat secara otomatis berdasarkan dari pengalaman sebelumnya [3].

Terdapat beberapa jurnal yang melakukan penelitian tentang *web phishing*, seperti jurnal yang berjudul *Phising Website Detection Using Machine Learning* [4], *Phishing Website Detection Based on Machine Learning: A Survey* [5], *Phishing Website Detection Using Machine Learning* [6], *Phishing Website Detection Based on Effective Machine Learning Approach* [7], *An Effective Detection Approach For Phishing Websites Using URL and HTML Features* [8], Analisis Komparasi Algoritma Klasifikasi *Data Mining* Dalam Klasifikasi *Website Phishing* [9] dan Identifikasi *Website Phishing* dengan Perbandingan Algoritma Klasifikasi [10].

Pada penelitian ini, peneliti menggunakan *mechine learning* dengan memanfaatkan fitur filter yang terdapat di dalamnya. Salah satu fitur filter yang akan digunakan adalah *person correlation. Person correlation* adalah seleksi fitur yang mengukur hubungan linier antara 2 variabel [11]. Filter digunakan untuk memilih fitur *website phishing* dan setelah dilakukan filter maka akan dilakukan penerapan 3 metode pada *machine learning* yaitu *naïve bayes, decision tree* dan *random forest*. Tujuan dari penelitian ini adalah untuk menentukan metode yang paling efektif untuk mendeteksi *website phising*.

2. Metode Penelitian

Terdapat 4 alur penelitian yang akan digunakan, yaitu dimulai dari (1) Tahap persiapan, (2) Metode yang akan digunakan, (3) Analisa dan (4) Evaluasi, seperti dijelaskan pada Gambar 1.



Gambar 1 Tahap Penelitian

Pada tahap persiapan dilakukan dengan menyiapkan *dataset* yang sebelumnya sudah disispkan dengan cara menggunduh gratis melalui *website* UCI *Machine Learning* [12]. *Dataset* yang akan digunakan pada penelitian ini adalah *dataset* yang bersifat *benchmark* dan didalam *dataset* tersebut terdapat 11055 data dengan 30 fitur yang tersedia, seperti yang ditunjukan pada Tabel 1 [13].

TABEL 1 FITUR WEBSITE PHASHING

Section	Nama Fitur	Deskripsi
Address Bar Based Faeture	*Having IP Address*	Website akan terindikasi website phishing ketika menggunakan IP Address atau menggunakan hexadecimal
	URL Lenght	Wesbite akan terindikasi sebagai website phishing ketika panjang dari URL addressnya sekitar 54 karakter
	Shortining Service	Website akan terindikasi website phishing ketika menggunakan short URL seperti “TinyURL”
	Having at (@) Symbol	Website akan terindikasi website phishing ketika URL website mengandung simbol “@”
	Double Slash (//) Redirecting	Website yang tidak terindikasi phishing letak dari “//” berbeda untuk HTTP dan HTTPS. HTTP terletak di karakter nomor 6 sementara HTTPS terletak di karakter nomor 7
	Prefix Suffix	Website yang terindikasi website phishing yang mengandung suatu prefix atau suffix di dalam URL address
	Having S ubDomain	Website yang terindikasi phishing, domain dan sub domain terlalu banyak dot (.) di URLaddress
	SSL Final State	Jika website menggunakan HTTPS dan sertifikat tidak kadaluarsa maka website tersebut kemungkinan bukanwebsite phishing
	Domain Registration Length	Website yang terindikasi phishing adalah ketika mempunyai domain yang singkat dan tidak lama

Section	Nama Fitur	Deskripsi
		seperti website yang terpercaya
	Favicon	Jika favicon di ambil dari domain luar (external domain) maka terindikasi website phishing
	Port	Jika ada port yang terbuka selain menggunakan port HTTP (80), maka website tersebut merupakan indikasi adanya phishing
	HTTPS Token	Website yang terindikasi phishingtidak mempunyai token autentikasi seperti website yang terpercaya
	Request URL	Website yang terpercaya, semua media berada didalam satu URL dan domain yang sama
	URL of Anchor	Anchor adalah suatu tag <a> yang mereprentasikan berapa banyak yang terhubung ke link URL lainnya, semakin banyak maka website tersebut terindikasi phishing
Abnormal Based Feature	*Links in Tags*	Website yang terpercaya menggunakan <meta> tag untuk metadata, <script> untuk membuat client-side script, dan <link> untuk menghubungkan ke link lainnya
	SFH (Server form Handler)	Jika domain URL menggunakan SFH yang blank (tidak diisi) atau menggunakan domain yang berbeda
	Submitting to Email	Website yang terindikasi phishingmengirimkan link website menggunakan email yang tidak terpercaya
	Abnormal URL	Website yang terpercaya diidentifikasi dengan menggunakan WHOIS database yang sebelumnya sudah terdaftar
	Redirect	Website yang terindikasi phishing semakin banyak melakukan redirectURL
	On Mouseover	Website phishing menggunakan event untuk mengubah status bar
HTML and Javascript Based Feature	*Right Click*	Website phishing menonaktifkan klik kanan agar tidak bisamelihat source page
	Pop Up Window	Website phishing terdapat pop up windows yang mencurigakan
	Iframe	Website phishing menyembunyikan halaman lain secara tersembunyi agar tidak terlihat
	Age of Domain	Umur domain untuk website sekitar 6 bulan
	DNS Record	DNS yang tidak ada di database WHOIS terindikasi phishing
	Web Traffic	Website phishing mempunyai traffic yang mencurigakan
Domain Based Feature	*Page Rank*	95% website Phishin tidak terdapat di page rank pencarian
	Google Index	Website yang terpercaya akan terindex google
	Link Pointing to Page	Website terpercaya akan menampilkan hubungan dengan website lainnya
	Statistical Report	Tergantung dari laporan perodik sehingga mengetahui beberapa websitephishing

Dapat dilihat pada Tabel 1, terdapat 4 karakteristik *phishing*, yaitu *Address Bar Based Feature, Abnormal Based Feature, HTML and Javascript Based Feature* dan *Domain Based Feature*. Pada hasil akhir akan didaptakan 3 *value*, *value* 1 mengidentifikasi *website* tersebut bebas dari *phashing*, *value* 0 mengidentifikasi *website* tersebut mencurigakan dan *value* -1 mengidentitifikasi *website phashing*. Dalam *dataset* ini dilakukan filter menggunakan *pearson correlation*. Nilai yang dihasilkan pada *pearson correlation* terletak pada [-1;1], dimana nilai -1 berarti korelasi negative sempurna, jika +1 berarti korelasi positif sempurna dan 0 berarti tidak ada korelasi linier antara kedua variable tersebut [14]. Nilai *pearson correlation* dapat dihitung menggunakan rumus persamaan (1).

$$r_{xy} = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)2}\sqrt{\sqrt{n\sum y_i^2 - (\sum y_i)2}}} \quad (1)$$

Filter *pearson correlation* yang diambil yaitu yang hasilnya diatas 0.1 atau *pearson correlation* > 0.1 sehingga terdapat fitur yang sesuai pada Tabel 2.

TABEL 2 HASIL FILTER *PEARSON CORRELATION*

Nama Fitur	Hasil Pearson Correlation
Prefix Suffix	0.348606
Having Sub Domain	0.298323
SSL Final State	0.714741
Domain Registratin Length	0.225789
Request URL	0.253372
URL of Anchor	0.692935
Links in Tags	0.248229
SFH	0.221419
Age of Domain	0.121496
Web Traffic	0.346103
Page Rank	0.104645

Pada Tabel 2, terdapat 12 fitur setelah di lakukan filter menggunakan *pearson correlation*, selanjutnya data akan dipisah menjadi *data training* dan *data testing* dengan bobot 70% untuk *data training* dan 30% untuk *data testing*. Pada tahap selanjutnya akan masuk ke dalam tahap metode yang

digunakan serta analisis.Terdapat 3 metode yang akan digunakan pada penelitian ini, yaitu:

2.1 Naïve Bayes

Naïve bayes classifier ditemukan oleh seorang ilmuan Inggris Bernama Thomas Bayes, naïve bayes classifier merupakan metoda pembelajaran mesin yang memanfaatkan perhitungan probabilitas dan statistik. Naïve bayes adalah salah satu algoritma di dalam *machine learning* dengan metode klasifikasi yang berkaitan dengan toerema bayes. Metode ini cocok digunakan untuk menentukan dan mendeteksi adanya *website phising*. Naïve bayes dirumuskan pada persamaan (2) [15].

$$P\ (H|X) = \frac{P(X|H)}{P(X)}\ .P(H) \quad (2)$$

Dimana,

X : Data dengan class yang belum diketahui

H : Hipotesis data menrupakan suatu class spesifik

P(H|X) : Probabilitas hipotesis H berdasarkan kondisi X

P(H) : Probabilitas hipotesis H

P(X|H) : Probabilitas hipotesis X berdasarkan kondisi H

P(X) : Probabilitas X

2.2 Decision Tree

Decision tree atau Clasification and Regression Tree (CRT) adalah seuatu algoritma pada *machine learning* yang memiliki fungsi untuk mengekplorasi data serta menemukan hubungan dari beberapa data yang ada di dalam *dataset*. Perhitungan di dalam *decision tree* berkaitan dengan *Entropy* dan *Gain.Entropy*, di rumuskan pada persamaan (3) dan (4) [16].

$$Gain(S,A) = Enthropy(S) - \sum_{i=1}^{n} \frac{|s_i|}{|s|} * Entropy(s_i) \quad (3)$$

Dimana,

S : Himpunan kasus

A : Atribut

N : Jumlah partisi atribut A

|Si| : Jumlah kasus pada partisi ke-i

|S| : Jumlah kasus dalam S

Sementara itu, perhitungan nilai *entropy* dapat dilihat pada persamaan (4) berikut.

$$Entropy(S) = \sum_{i=1}^{n} -pi * log_2\ pi \quad (4)$$

Dimana,

S : Himpunan kasus

A : Fitur

n : Jumlah partisi S

pi : Proporsi dari Si terhadap S

2.3 Random Forest

Random forest adalah sebuah algoritma yang berkerja dengan membuat sejumlah pohon klasifikasi secara acak. Pohon-pohon tersebut dibuat dengan menggunakan sampel yang berbeda dari kumpulan data yang sama dan dapat menggunakan jenis fitur yang berbeda setiap membuat pohon, sehingga semua pohon dibuat secara acak dengan memanfaatkan subset berbeda dari kumpulan data yang sama dan fitur diambil secara acak untuk membuat sebuah pohon. Random forest adalah kombinasi dari *tree* yang ada di dalam decision tree, semakin banyak *tree* maka akan semakin baik tingkat akurasi hasilnya. Dengan melakukan hal tersebut, Random Forest memastikan bahwa data tidak *overhit*, seperti pada decision tree.

3. Hasil dan Pembahasan

Dataset website phishing dari UCI *Machine Learning* menjadi *dataset* untuk uji coba dalam penelitian ini, hal yang akan dilakukan pertama kali pada *dataset* ini adalah dilakukan filter menggunakan *pearson correlation*. Pengambilan *pearson correlation* lebih dari 0.1 sehingga *dataset* yang awalnya mempunyai 30 fitur, setelah dilakukan filter dengan *pearson correlation* menjadi 12 fitur. Selanjutnya dilakukan *testing* data sebanyak 30% menggunakan 3 metode model yaitu naïve bayes, decision tree dan random forest, sehingga didapatkan akurasi seperti yang ditunjukan pada Tabel 3.

TABEL 3 HASIL AKURASI

Metode	Akurasi
Naives Bayes	60,4 %
Decision Tree	94,4 %
Random Forest	96,3 %

Berdasarkan hasil nilai akurasi yang ditunjukan pada Tabel 3, nilai akurasi pada masing-masing metode memiliki hasil yang berbeda. Pada metode naïve bayes memiliki nilai akurasi sebesar 60,4%, metode decision tree memiliki nilai akurasi 94,4% dan metode random forest memiliki akurasi sebesar 96,3%. Sehingga dapat disimpulakan bahwa metode yang paling efektif untuk mendeteksi website phishing adalah menggunakan random forest karena memiliki tingkat akurasi sebesar 96.3%

4. Kesimpulan

Penerapan metode random forest merupakan algoritma yang paling efektif mendeteksi website phishing setelah dilakukan filter menggunakan pearson correlation karena memiliki tingkat akurasi sebesar 96,3%. Untuk penelitian selanjutnya dapat dilakukan pada kasus yang sama, akan tetapi menggunakan algoritma yang lainnya untuk menemukan algoritma yang lebih baik.

Daftar Pustaka

[1] S. H. Wibowo *et al.*, *Cyber Crime Di Era Digital*. Sumatra Barat: Pt Global Eksekutif Teknologi , 2022.

[2] P. D. Kusuma, *Machine Learning Teori, Program dan Studi Kasus*. Yogyakarta: Cv Budi Utama, 2022.

[3] T. M. Mitchell, *Machine Learning*. New York: In McGraw Hill Series in Computer Science, 1997.

[4] R. Kiruthiga and D. Akila, "Phishing Website Detection Using Machine Learning," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2S11, Sep. 2019.

[5] C. Singh and Meenu, "Phishing Website Detection Based on Machine Learning: A Survey," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Mar. 2020.

[6] A. Mandadi, S. Boppana, V. Ravella, and R. Kavitha, "Phishing Website Detection Using Machine Learning," in *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, IEE, Apr. 2022.

[7] G. H. Lokesh and G. Boregowda, "Phishing website detection based on effective machine learning approach," *Journal of Cyber Security Technology*, pp. 1–14, Aug. 2020, doi: https://doi.org/10.1080/23742917.2020.1813396.

[8] A. Aljofey *et al.*, "An Effective Detection Approach For Phishing Websites Using URL and HTML Features," *Sci Rep*, May 2022.

[9] N. B. Putri and A. W. Wijiyanto, "Analisis Komparasi Algoritma Klasifikasi Data Mining Data Mining Dalam Klasifikasi Website Phishing," *Komputika: Jurnal Ssitem Komputer*, vol. 11, pp. 59–66, Apr. 2022.

[10] A. S. Y. Irawan, N. Heryana, H. S. Hopipah, and D. R. Putri, "Identifikasi Website Phishing dengan Perbandingan Algoritma Klasifikasi," *SYNTAX: Jurnal Informatika*, vol. 10, pp. 57–67, May 2021.

[11] P. Samuels and M. Gilchrist, *Pearson Correlations*. Affiliation: Birmingham City University, 2014.

[12] "Phishing Websites," *UCI Machine Learning*, Feb. 2015. https://archive.ics.uci.edu/dataset/327/phishing+websites (accessed Aug. 03, 2023).

[13] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Phishing Websites Features," in *International Conferece For Internet Technology And Secured Transactions (CITST)*, London, UK, 2012, pp. 492–497.

[14] F. R. S. Rangkuti, M. A. Fauzi, Y. A. Sari, and E. D. L. Sari, "Analisis Sentimen Opini Film Menggunakan Metode Naïve Bayes dengan Ensemble Feature dan Seleksi Fitur Pearson Correlation Coefficient," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, pp. 6354–6361, Dec. 2018.

[15] A. Fatkhurohman and E. Pujastuti, "Penerapan Algoritma Naive Bayes Classifier Untuk Meningkatkan Keamanan Data Dari Website Phising," *Jurnal Teknologi Informasi*, vol. XIV, Mar. 2019.

[16] E. T. Luthfi and Kusrini, *Algoritma Data Mining*. Yogyakarta: CV ANDI OFFSET, 2009.