ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.1 No.1 Tahun 2022
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-1 2022
Fakultas Teknik, Universitas Pelita Bangsa, Juli 2022

Komparasi *Machine Learning* Memprediksi Phising Dalam Keamanan *Website*

Machine Learning Comparison Predicting Phishing in Website Security

Aswan Supriyadi Sunge[1]
[1]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]aswan.sunge@pelitabangsa.ac.id

Abstract

The growth rate of online mobility is fast and increases sharply from desktop to mobile phone. Growth is recognized by users because of the ease of searching for information and dealing mainly in banking matters. Behind them, there is the most important issue of security on the Internet, one of them Phishing which means to resemble official or original websites when false with the intention of obtaining user information. There fore it takes a malicious web-based Phishing alias by using data set, then tested with some Machine Learning algorithms and then to compare the best and highest predictions. Computer simulation results have resulted an accuracy of up to 95.24% for the techniques used and the comparison with other models.

***Keywords**: Predictions, Website, Phishing, Machine Learning*

Abstrak

Tingkat pertumbuhan mobilitas online cepat dan meningkat tajam dari desktop ke ponsel. Pertumbuhan diakui oleh pengguna karena kemudahan mencari informasi dan berurusan terutama dalam hal perbankan. Di belakang mereka, ada masalah keamanan yang paling penting di Internet, salah satunya Phishing yang berarti menyerupai situs web resmi atau asli ketika palsu dengan tujuan untuk mendapatkan informasi pengguna. Oleh karena itu dibutuhkan sebuah web-based Phishing alias dengan menggunakan dataset, kemudian diuji dengan beberapa algoritma Machine Learning kemudian untuk membandingkan prediksi terbaik dan tertinggi. Hasil simulasi komputer telah menghasilkan akurasi hingga 95,24% untuk teknik yang digunakan dan perbandingan dengan model lain.

Kata Kunci: Prediksi, Website, Phishing, Pembelajaran Mesin.

Pendahuluan

Dalam dua dekade terakhir, jumlah pengguna internet di seluruh dunia meningkat secara signifikan [1]. Pertumbuhan ini juga dibarengi dengan penggunaan e-commerce yang menyediakan belanja online, pertukaran data elektronik, dan transaksi perbankan. Sayangnya, di balik kemudahan dalam berinternet tersebut muncul kejahatan dunia maya termasuk berbagai perilaku ilegal yang mengarah pada sistem keamanan dari sistem komputer sasaran [2]. Munculnya kejahatan dunia maya sebagian besar karena ketidaktahuan pengguna internet tentang keamanan internet atau tidak dapat membedakan situs yang aman [3] dan media sosial Internet [4].

Phising adalah istilah yang mengacu pada berbagai tindakan *cybercrime* dengan memberikan *link* ke pengguna internet yang bertujuan untuk mencuri data pribadi seperti bank, PIN dan data di media sosial[5]. Metode umum yang digunakan dalam penipuan pengguna online adalah menyediakan tautan atau pesan email. Aktivitas phising telah mendapatkan minat penelitian di kalangan komunitas keamanan internet karena seringkali sulit bagi pengguna untuk mengenali tindakan tersebut [6]. Oleh karena itu, penelitian ini bertujuan untuk memprediksi situs yang terindikasi aman atau tidak aman saat dikunjungi.

Data mining adalah kumpulan metode untuk mempelajari pola dari data masa lalu [7]. Diantara permasalahan yang dapat dipecahkan dengan menggunakan teknik data mining adalah klasifikasi [8][9]. Tujuan dari klasifikasi adalah untuk memprediksi secara akurat kelas yang dicari pada setiap kasus dalam data [10].

Model Pembelajaran Mesin

Phising web adalah topik penelitian yang telah mendapatkan minat penelitian yang menghasilkan sejumlah besar publikasi. Di antara metode yang diusulkan untuk mengatasi phising web adalah model pembelajaran mesin [11][12][13]. Model klasifikasi dapat dilatih menggunakan teknik pelatihan *unsupervised* [14], *semi-supervised* [15], *supervised* [16][17][6]. Pembelajaran mesin terdiri dari model untuk belajar dari dataset pelatihan untuk membuat prediksi yang akurat tentang data baru [18][19]. Meskipun banyak model pembelajaran mesin telah diusulkan, banyak penelitian sebelumnya menunjukkan bukti bahwa tidak ada model tunggal akan memastikan kinerja tinggi untuk setiap dataset [20][21][22][23].

1. *Decision Tree*
   Model pohon keputusan banyak digunakan untuk pendeteksian web phishing [5][24]. Salah satu algoritma pembuatan pohon keputusan yang menonjol adalah algoritma C4.5. Keuntungan dari algoritma pohon keputusan adalah kemampuannya untuk menangani atribut kontinu dan data yang hilang. Dalam penelitian ini, pemilihan fitur dalam pembuatan pohon keputusan didasarkan pada Gain Ratio untuk mengurangi bias terhadap atribut multi-nilai yang dapat dihitung sebagai berikut:

$$GainRatio(S,A) = \frac{Gain(S.A)}{SplitInfo(S.A)} \quad (1)$$

   Dimana:
   S = Space/Sampel Data yang digunakan untuk Data Training
   A = atribut
   Gain (S,A) = Dapatkan informasi tentang atribut A
   SplitInfo (S,A) = membagi informasi pada atribut A
   Setelah dihitung, atribut tertinggi nilai Gain Ratio digunakan sebagai atribut uji untuk node. Pendekatan ini mengimplementasikan normalisasi perolehan informasi yang disebut split information dengan rumus:

$$SplitInfo(S.A) = -\sum_{i=1}^{i} \frac{S_i}{s} log_2 \frac{S_i}{s} \quad (2)$$

   Dimana:
   S = Space/Sampel Data yang digunakan untuk Data Training
   A = atribut
   Si = Jumlah sampel untuk atribut i
   Data yang hilang pada input dataset ditangani dengan teknik pruning [25] berdasarkan rumus berikut:

$$e = \frac{r + \frac{Z^2}{2_n} + Z\sqrt{\frac{r}{n} - \frac{r^2}{n} + \frac{Z^2}{4n^2}}}{1 + \frac{Z^n}{n}} \quad (3)$$

   Dimana:

   R = nilai perbandingan tingkat kesalahan
   n = jumlah sampel
   z = ϕ^{-1} *(c)*
   c = tingkat kepercayaan

2. *Naïve Bayes (NB)*
   Model klasifikasi berdasarkan teori probabilitas dan teorema Bayesian [26]. Salah satu kelebihan NB adalah mengandalkan bahwa tidak ada atribut tersembunyi yang dapat mempengaruhi dalam proses prediksi.

3. *Multilayer Perceptron (Neural Network)*
   Neural Network (NN) adalah model yang banyak digunakan untuk klasifikasi. Model ini terinspirasi oleh *neurofisiologi* otak manusia melalui kombinasi elemen komputasi sederhana (neuron) dalam sistem

yang saling berhubungan. Salah satu keunggulan NN adalah kemampuannya dalam menangani data yang mengandung *noise* [7]. *Multilayer perceptron* (MLP) juga dikenal sebagai *Multilayer Feedforward Neural Network* adalah algoritma yang paling banyak digunakan. MLP terdiri dari satu lapisan input, satu atau lebih lapisan tersembunyi, dan satu lapisan outpun [27].

4. *K-Nearest Neighbor (K-NN)*
   K-NN adalah algoritma pembelajaran terawasi dimana hasil dari instance baru diklasifikasikan oleh mayoritas kategori tetangga terdekat. Tujuan dari algoritma ini adalah untuk mengklasifikasikan objek baru berdasarkan atribut dan sampel dari data training. Algoritma K-NN menggunakan *Neighborhood Classification* sebagai nilai prediksi dari nilai *instance* baru [28].

5. *Support Vector Machines (SVM)*
   SVM yang ditemukan oleh Vapnik sejak itu telah banyak digunakan dalam studi penelitian terutama dalam pembelajaran mesin [28]. Beberapa penelitian terbaru melaporkan bahwa SVM secara umum mampu memberikan kinerja dalam hal akurasi klasifikasi dari algoritma klasifikasi data lainnya. SVM telah digunakan dalam berbagai masalah dunia nyata seperti kategorisasi teks, tulisan tangan, pengenalan digit, pengenalan nada dan deteksi objek. Terbukti SVM konsisten mengungguli metode pembelajaran lain yang disupervisi. Namun, untuk beberapa kumpulan data, kinerja SVM sangat sensitif terhadap bagaimana parameter biaya dan parameter kernel ditetapkan. Akibatnya, pengguna biasanya perlu melakukan validasi silang ekstensif untuk mengetahui pengaturan parameter yang optimal.

Metode Penelitian

Dataset

Data yang digunakan dikumpulkan dari dataset situs web phishing. Data dikonversi dalam format .csv untuk memudahkan analisis. Jumlah sampel untuk input dataset adalah 11.055 data dengan 30 atribut. Data dikategorikan sebagai Kelas aman (-1) dan tidak aman (1).

Untuk model training phising klasifikasi, seluruh data dibagi secara acak menjadi 2 bagian yang digunakan sebagai data training 80% berjumlah 8.844 data dan data testing 20% berjumlah 2.211 data. Nilai atribut kelas berkisar dari -1, 0 dan 1. Nilai tersebut mewakili kekuatannya mulai dari rendah, sedang dan tinggi.

Tabel 1 Atribut dan Nilai Dataset

Attribute	Values
having_IP_Address	{-1, 1}
URL_Length	{-1, 0, 1}
Shortining_Service	{-1, 1}
having_At_Symbol	{-1, 1}
double_slash_redirecting	{-1, 1}
Prefix_Suffix	{-1, 1}
having_Sub_Domain	{-1, 0, 1}
SSLfinal_State	{-1, 1, 0}
Domain_registeration_length	{-1, 1}
Favicon	{-1, 1}
Port	{-1, 1}
HTTPS_token	{-1, 1}
Request_URL	{-1, 1}
URL_of_Anchor	{-1, 0, 1}
Links_in_tags	{-1, 1, 0}
SFH	{-1, 1, 0}
Submitting_to_email	{-1, 1}
Abnormal_URL	{-1, 1}
Redirect	{0, 1}
on_mouseover	{-1, 1}
RightClick	{-1, 1}
popUpWidnow	{-1, 1}

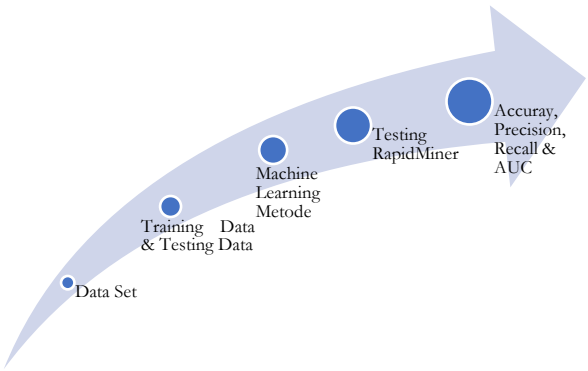
Attribute	Values
Iframe	{-1, 1}
age_of_domain	{-1, 1}
DNSRecord	{-1, 1}
web_traffic	{-1, 0, 1}
Page_Rank	{-1, 1}
Google_Index	{-1, 1}
Links_pointing_to_page	{-1, 1}
Statistical_report	{-1, 0, 1}
Class	{-1, 1}

Data Preprocessing

Data yang diunduh dalam formulir. format csv. Setiap atribut sudah memiliki nama atribut dan bukan nilai kosong. Oleh karena itu, tidak perlu dilakukan preprocessing data dan kumpulan data yang akan digunakan untuk analisis.

Model Training

Tahapan dalam penelitian ini dilakukan dalam web phishing berdasarkan metode Machine Learning, yang dijelaskan sebagai berikut.



Gambar 1 Metodologi Deteksi Situs Web Phishing Berbasis Machine Learning

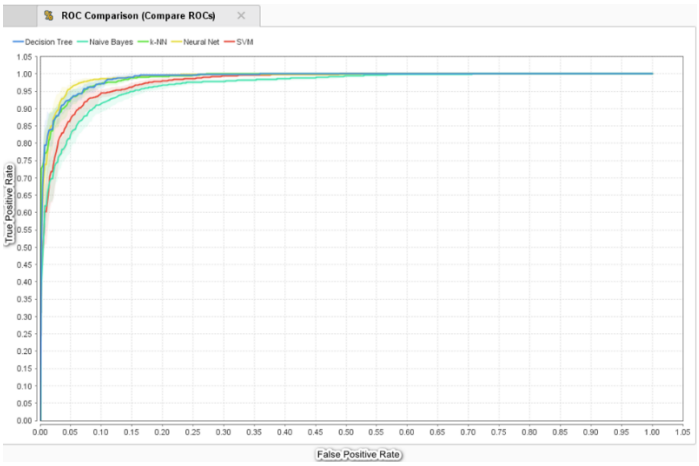
Hasil dan Pembahasan

Jika dilihat dari kelima metode dengan testing RapidMiner Studio, maka akurasi tertinggi dari data training dan testing adalah Neural Network dan K-NN. Keakuratan model classifier yang dieksplorasi dalam penelitian ini dapat diringkas dan dilihat pada Tabel 2 berikut :

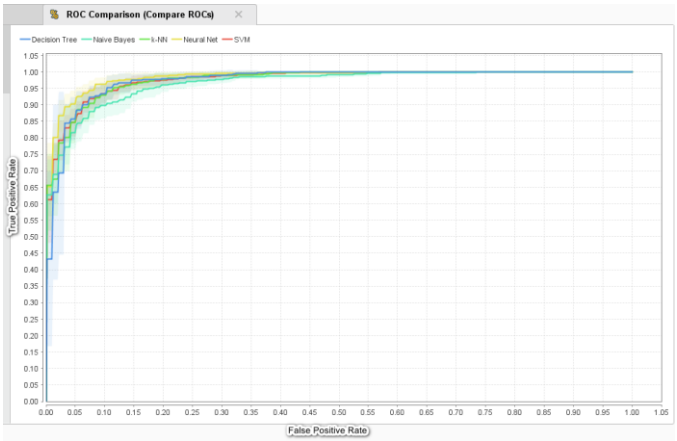
Tabel 2 Ringkasan Kinerja Model

Model	Training Accuracy	Training Precision	Training Recall	Training AUC	Testing Accuracy	Testing Precision	Testing Recall	Testing AUC
Decision Tree (C4.5)	93.33%	94.39%	93.62%	0.983	91.77%	92.99%	92.36%	0.963
Naive Bayes	72.56%	99.29%	51.01%	0.968	72.73%	99.69%	51.62%	0.967
Multilayer Perceptron (NN)	95.17%	95.17%	96.22%	0.989	92.85%	93.70%	93.64%	0.981
K-Nearest Neighbor	93.72%	94.12%	94.63%	0.980	91.81%	92.28%	92.31%	0.967
Support Vector Machine	92.15%	91.27%	94.98%	0.977	91.81%	90.87%	95.09%	0.977

Hasil yang didapatkan pada kurva ROC didapatkan hasil yang tidak jauh berbeda dengan Neural Network dari data latih atau pengujian dan hasilnya pada Gambar 2 dan Gambar 3 berikut :



Gambar 2 Perbandingan ROC tertinggi dari lima metode dengan Data Training



Gambar 3 Perbandingan ROC tertinggi dari lima metode dengan Data Testing

Kesimpulan

Dari hasil penelitian ini dengan lima metode machine learning dan hasil pengujian menunjukkan bahwa memiliki akurasi tertinggi dalam memprediksi web phishing. Semua metode membentuk teknik-teknik terawasi dan dibagi menjadi dua kelas. Dari kelima metode tersebut ternyata Neural Network lebih tinggi untuk mendeteksi phishing.

Daftar Rujukan

[1] M. M. Group., (2019), "Internet Usage in Asia," [Online]. Available: https://www.internetworldstats.com/stats3.htm. [Accessed: 17-Jul-2019].

[2] P. B. Pathak, (2016), "Cybercrime : A Global Threat to Cybercommunity," Ijcset.Com, vol. 7, no. 03, pp. 46–49, 2016.

[3] M. M. Kamal, I. A. Chowdhury, N. Haque, M. I. Chowdhury, and M. N. Islam, (2012), "Nature of cyber crime and its impacts on young people: A case from Bangladesh," *Asian Soc. Sci.,* vol. 8, no. 15, pp. 171–183.

[4] F. Salahdine and N. Kaabouch, (2019), "Social Engineering Attacks: A Survey," *Futur. Internet,* vol. 11, no. 4, p. 89.

[5] L. MacHado and J. Gadge, (2018), "Phishing Sites Detection Based on C4.5 Decision Tree Algorithm," 2017 *Int. Conf. Comput. Commun. Control Autom. ICCUBEA* 2017, pp. 1–5.

[6] A. S. Sunge, (2018), "Optimasi Algoritma C4.5 Dalam Prediksi Web Phishing Menggunakan Seleksi Fitur Genetic Algoritma," *Paradigma*, vol. 10, no. 2, pp. 27–32.

[7] D. T. Larose, (2015), Discovering Knowledge in Data: An Introduction to Data Mining. John Willey & Sons, Inc.

[8] S. Neelamegam and E. Ramaraj, (2013), "Classification algorithm in Data mining : An Overview," vol. 3, no. 5, pp. 1–5.

[9] S. Asiri, (2018), "Machine Learning Classifiers," Towards Data Science, [Online]. Available:

https://towardsdatascience.com/machine-learning-classifiers-a5cc4e1b0623. [Accessed: 20-Jun-2019].

[10] G. Kesavaraj and S. Sukumaran, (2013), "A study on classification techniques in data mining," in 2013 4th International Conference on Computing, Communications and Networking Technologies, *ICCCNT 2013,* pp. 1–7.

[11] E. A. Kaur, (2016), "Detection of Phishing Websites Using Data Mining Techniques," *Int. J. Eng. Res. Technol.*, vol. 2, no. 8, pp. 1273–1276.

[12] A. S. Sunge, (2018), "Optimasi Algoritma C4.5 Menggunakan Genetic Algoritma Dalam Memprediksi Website Phishing," *in Seminar Nasional Inovasi dan Tren (SNIT),* p. 92.

[13] M. Dedakia and K. Mistry, (2015), "Phishing Detection using Content Based Associative Classification Data Mining," *J. Eng. Comput. Appl. Sci.,* vol. 4, no. 7, pp. 209–214.

[14] R. Layton, P. Watters, and R. Dazeley, (2012), "Unsupervised Authorship Analysis of Phishing Webpages," pp. 1104–1109..

[15] Y. Li, R. Xiao, J. Feng, and L. Zhao, (2013), "A semi-supervised learning approach for detection offphishing webpages," *Elsevier*, vol. 124, no. 23, pp. 6027–6033.

[16] V. S. Lakshmi and M. S. Vijaya, (2012), "Efficient prediction of phishing websites using supervised learning algorithms," *Procedia Eng.*, vol. 30, no. 2011, pp. 798–805.

[17] W. Ali, (2017), "Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection," *(IJACSA) Int. J. Adv. Comput. Sci. Appl.,* vol. 8, no. 9, pp. 72–78.

[18] R. Schapire, Machine Learning Algorithms for Classification. Princeton University.

[19] Wiyanto, W., Fadhilah, S., & Siswandi, A. (2022). E-Tourism Sebagai Media Wisata Kabupaten Bekasi Berbasis Website. *Journal of Practical Computer Science*, *2*(1), 1-14.

[20] F. Gharehchopogh and Y. Lotfi, (2013), "Machine Learning based Question Classification Methods in the Question Answering Systems," *Int. J. Innov. …,* vol. 4, no. 2, pp. 264–273.

[21] Https://medium.com, (2019), "Types of classification algorithms in Machine Learning," [Online]. Available: https://medium.com/@Mandysidana/machine-learning-types-of-classification-9497bd4f2e14. [Accessed: 18-Jun-2019].

[22] P. Glauner et al., (2017), "The Top 10 Topics in Machine Learning Revisited: A Quantitative Meta-Study," no. April.

[23] Stephanie Glen, (2019), "Comparing Classifiers: Decision Trees, K-NN & Naive Bayes," Data Science Central., 2019. [Online]. Available: https://www.datasciencecentral.com/profiles/blogs/comparing-classifiers-decision-trees-knn-naive-bayes?fbclid=IwAR2UiaGgxdcWYffAvCLfMrsR2f8cSh10-IGQ-ce99tYaIxT7OCH286VMQ7c. [Accessed: 19-Jun-2019].

[24] S. K. Shinde, (2017), "Detection of Phishing Websites Using C4.5 Data Mining Algorithm," *Int. Conf. Recent Trends Electron. Inf. Commun. Technol.,* vol. 2, no. 12, pp. 3725–3729, 2017.

[25] A. S. Sunge, (2018), "Prediksi Kompetensi Karyawan Menggunakan Algoritma C4. 5 (Studi Kasus : PT Hankook Tire Indonesia)," vol. 2018, no. *Sentik*a, pp. 23–24.

[26] I. H. & F. E. Witten, (2000), "Data Mining– Practical Machine Learning Tools and Techniques," *Second edi., M. Kaufmann, Ed. San Francisco*.

[27] C. Vercellis, (2009), Business Intelligence: Data Mining and Optimization for Decision Making. United Kingdom.

[28] A. M. Ismail, (2018), "Cara Kerja Algoritma k-Nearest Neighbor (k-NN)," https://medium.com. [Online]. Available: https://medium.com/bee-solution-partners/cara-kerja-algoritma-k-nearest-neighbor-k-nn-389297de543e. [Accessed: 21-Jun-2019].

[29] H. Wang, Y. Shi, X. Zhou, Q. Zhou, S. Shao, and A. Bouguettaya, (2010), "Web service classification using support vector machine," *Proc. - Int. Conf. Tools with Artif. Intell. ICTAI,* vol. 1, pp. 3–6.