View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Repository Proceeding Seminar (Fakultas Ilmu Komputer, Universitas Sriwijaya)

ARS 2018 The 4th Annual Research Seminar
Prosiding Annual Research Seminar 2018
Computer Science and ICT
ISBN : 978-979-587-813-1
Vol.4 No.1

Klasifikasi *Malicious Website* Menggunakan Metode Algoritma *K-Nearest Neighbor* (KNN)

Nadhya Hassni[1]
Fakultas Ilmu Komputer
Universitas Sriwijaya
Palembang, Indonesia
[1]nadhyahassni@gmail.com

Fidya Rianti Putri[2]
Fakultas Ilmu Komputer
Universitas Sriwijaya
Palembang, Indonesia
[2]riantiputrifidya@gmail.com

Abstrak - Saat ini malicious website mengalami perkembangan dalam beberapa waktu terakhir. Perkembangan infrastruktur perangkat lunak terjadi secara besar-besaran dan mempermudah para pelaku kejahatan malicious website untuk melakukan serangan. Pada paper ini dilakukan klasifikasi terhadap malicious website menggunakan K-Nearest Neighbor (KNN). Jumlah parameter yang digunakan dalam klasifikasi sebanyak 14 parameter dengan satu output yang mengidentifikasikan sebuah website malicious atau tidak. Tingkat akurasi yang dihasilkan cukup memuaskan dengan nilai sebesar 92.2% pada nilai K=3.

Kata Kunci- Klasifikasi, Malicious website, K-Nearest Neighbor.

I. PENDAHULUAN

Dikehidupan *modern* seperti sekarang dimana kemajuan teknologi sudah maju dengan pesat dan teknologi sudah mulai mencangkup semua aspek kehidupan. Bisa kita lihat setiap aspek kehidupan di dunia ini sudah menggunakan teknologi dan juga digunakan dalam berbagai bidang seperti pendidikan, pemerintahan, kesehatan dan lain-lain.

Dalam menerapkan teknologi tidak semua orang menggunakannya dengan landasan yang baik dan positif banyak juga orang yang menggunakan teknologi untuk melakukan tindak kriminal bahkan melakukan perniagaan ilegal dengan tujuan meraup keuntungan yang sebesar-besarnya dengan cara yang tidak benar.

Website juga berfungsi sebagai media untuk sejumlah besar aktifitas berbahaya seperti, *spam attack*, *pinising attacks*, *DDos attack* dan lain-lain, yang berpacu untuk aspek finansial[1]. *Cybercrime* telah mengalami perkembangan dalam beberapa waktu terakhir, disebabkan dengan perkembangan infrastruktur perangkat lunak yang terjadi secara besar-besaran, mempermudah para pelaku untuk melakukan serangan[2].

Hal diatas merupakan skema umum untuk menghasilkan uang dengan cara pemasangan perangkat lunak yang berbahaya pada sejumlah alamat website, dalam mode ini alamat website yang terinfeksi akan membentuk potnet yang jaringannya diatur langsung dibawah kendali penjahat dunia maya[3]. Dalam tulisan ini, kami berfokus pada bagian klasifikasi keamanan pada kualitas hubungan URL dengan alamat website. Dengan motivasi memberikan cakupan yang lebih baik saat mengakses sebuah website[4].

Malicious website cukup sulit untuk di klasifikasikan dan di bedakan secara langsung, dikarenakan oknum-oknum yang terlibat membuat website-website tersebut menjadi seperti website yang biasa kita gunakan sehari-hari dan tanpa ciri yang bisa dilihat secara kasat mata . Dikarenakan kesulitan inilah sangat di butuhkan cara atau metode yang dapat mengklasifikasikan mana website yang baik dan *malicious website.*

Disalah satu riset yang pernah dilakukan sebelumnya dimana peneliti melakukan percobaan dengan metode statistik yang menggunakan mesin *learning* untuk mengklasifikasikan malicious website dengan hasil riset sebesar 95-99% dari 20000 sampai 30000 URL dengan hasil persentase yang besar ini terdapat kelemahan di mana terjadi ketidak stabilan dalam hasil persentase[4].

Dalam riset lain yang kami baca dengan menggunakan metode *algoritma batch* yang memeriksa website satu persatu dan terperinci untuk setiap sample website. Dalam riset ini pengklasifikasiannya menghasilkan nilai persentase sebesar 99% dan jauh lebih seimbang di banding penelitian yang kami bahas sebelumnya. Dengan besarnya hasil persentase dan keseimbangan riset ini

ISBN : 978-979-587-813-1
Vol.4 No.1

memakan waktu pemeriksan yang cukup lama di banding riset sebelumnya[5].

Dalam paper ini kami mencoba menggunakan metode KNN untuk mengklasifikasikan *malicious website* yang kami harapkan dapat menghasilkan persentase yang besar dan lebih seimbang di banding riset sebelumnya. Selain itu diharapkan dapat mengurangi waktu komputasi.

II. METODOLOGI

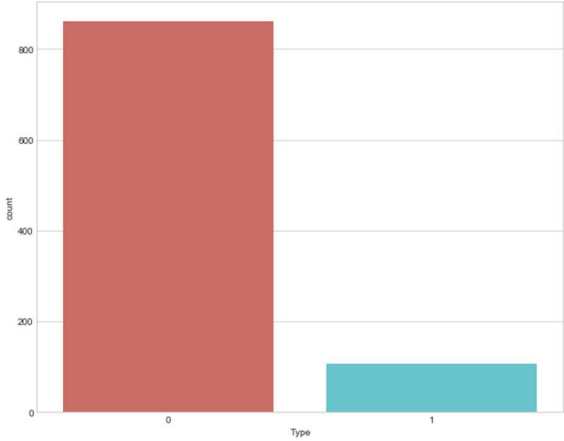
A. DataSet

Pada riset kali ini kami menggunakan data *malicious dan benign website* yang didapatkan dari *Kaggle*. Data ini memiliki 1000 data website dengan 14 parameter prediksi (Tabel I).

TABEL I. Parameter DataSet

Parameter	Keterangan
URL_LENGTH	Jumlah karakter url
NUMBER_SPECIAL_CHARCTERS	Jumlah spesial karakter dari URL seperti : "/","%","#","&",".","="
CHARSET	Standar dari encoding karakter
CONTENT_LENGTH	Besarnya konten dari HTTP
TCP_CONVERSATION_EXCHANGE	Jumlah pertukaran TCP packet antara server dan client
DIST_REMOTE_TCP_PORT	Jumlah dari port yang diketahui berbeda dari tcp
REMOTE_IPS	Jumlah dari IP yang terhubung
APP_BYTES	Jumlah byte yang ditransfer
SOURCE_APP_PACKETS	Paket yang dikirim ke server
REMOTE_APP_PACKETS	Paket yang diterimadaru server
SOURCE_APP_BYTES	Jumlah byte yang ditransfer ke server
REMOTE_APP_BYTES	Jumlah byte yang diterima dari server
APP_PACKETS	Jumlah IP yang di generate selama komunikasi antara honeypot dan server
DNS_QUENRY_TIMES	Jumlah DNS yang di generate selama komunikasi antara hpneypot dan server

Sedangkan untuk parameter respon kami menggunakan angka 1 (satu) dan 0 (nol). Jika bernilai 1 berarti website tersebut merupakan *malicious website* yang merupakan web palsu dan jika bernilai 0 maka website tersebut aman untuk di gunakan. Dengan pembagian data seperti grafik dibawah ini (Gambar 1)



Gambar .1. klasifikasi *website aman* dan *malicious website*

Dapat dilihat pada gambar diatas (Gambar 1) grafik dengan nilai 0 yang merupakan website yang aman dan bisa kita gunakan. Sedangkan grafik dengan dengan nilai 1 merupakan malicious website.

Bisa kita lihat bahwa dari 1000 data yang tersedia terdapat 900 data yang merupakan website aman dan 100 data yang merupakan malicious website.

B. K-Nearest Neighbor (KNN)

Algoritma KNN adalah sebuah metode yang digunakan untuk mengklasifikasikan objek berdasarkan data uji yang jaraknya paling dekat dengan objek tersebut. Algoritma ini terbagi menjadi dua jenis yaitu *algoritma supervised* dan *algoritma unsupervised.*

Algoritma supervised learning memiliki tujuan untuk menemukan pola baru dalam sebuah data dengan menghubungkan pola data yang sudah ada dengan data yang baru, sedangkan *unsupervised learning* adalah data yang belum memiliki pola apapun dan bertujuan untuk menemukan pola baru dalam data. Algoritma KNN termasuk salah satu metode yang menggunakan *algoritma supervised*[6]

C. Menghitung Jarak Kemiripan (K)

Pada penelitian ini jarak kemiripan dapat dihitung dengan menggunakan *minkowski*. *Minkowski* adalah jarak didalam ruang vektor yang sudah ditentukan dan

ISBN : 978-979-587-813-1
Vol.4 No.1

ISBN : 978-979-587-813-1
Vol.4 No.1

dianggap sebagai generalisasi dari kedua jarak *Euclidean* dan jarak *Manhattan*[7]

Jarak *minkowski* dapat digunakan untuk menghitung jarak dua buah vektor (a,b) yang didalamnya terdapat inisialisasi nilai p.

$$\mathbf{d}(\mathbf{x},\mathbf{y}) = \left(\sum_{i=1}^{n} |xi - yi|^{p}\right)^{1/p} \quad (1)$$

Pengukuran jarak *minkowski* meliputi *Manhattan/city block distance* dan *Euclidean distance, Manhattan/city bloch distance* (p=1), seperti pada persamaan 2

$$\mathbf{d}(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{n} |xi - yi| \quad (2)$$

Euclidean distance (p=2), seperti persamaan 3

$$\mathbf{d}(\mathbf{x},\mathbf{y}) = \sqrt{\sum_{k=1}^{n} (xi - yi)^{2}} \quad (3)$$

Keterangan :

d : Jarak
x : Titik awal
i : Jumlah data
y : Titik akhir
n : Banyak data

.

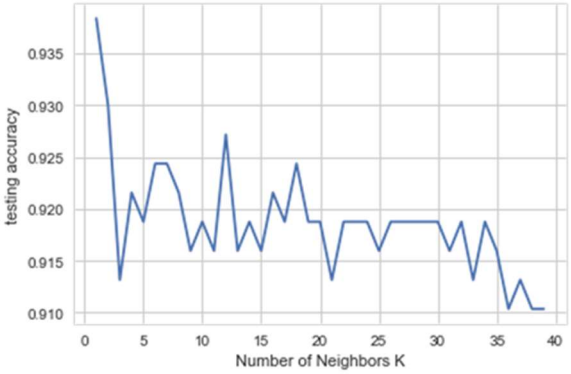
Metode KNN dilakukan dengan cara membandingkan data uji dengan data training. Tahap awal yang harus digunakan adalah menentukan nilai dengan *flow chart* seperti gambar di bawah ini (Gambar 2).

Gambar .2. Flow chart klasifikasi malicious website

III. HASIL DAN PEMBAHASAN

A. *Hasil Proses*

Untuk mendapatkan nilai K digunakan teknik validasi. Nilai K diuji dengan nilai 1 sampai dengan 40 . Dari hasil perhitungan nilai K terbaik adalah 3. Dengan ditetapkanya nilai K = 3 maka menghasilkan grafik seperti gambar dibawah ini(gambar 3).

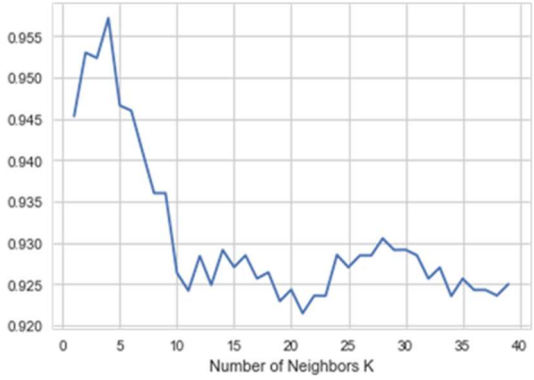


Gambar .3. testing akurasi

ISBN : 978-979-587-813-1
Vol.4 No.1

ISBN : 978-979-587-813-1
Vol.4 No.1

Setelah mendapatkan nilai K kami mulai menghitung untuk akurasinya seperti gambar dibawah ini



Gambar .4. cv_scores

Dari gambar 4 dapat ditentukan akurasi dari klasifikasi ini dengan menggunakan nilai K dengan nilai MSE (*Mean Square Error*) terendah. Pada grafik diatas dapat dilihat berbeda nilai K maka berbeda pula nilai akurasinya.

Pada gambar diatas ditentukan nilai MSE terendah untuk menentukan nilai akurasi. Dipilihnya nilai MSE terendah bertujuan agar akurasi yang dihasilkan lebih stabil dan memiliki nilai eror yang rendah. Ditemukan bahwa nilai K dengan MSE terendah adalah 21 dan dari nilai tersebut didapat nilai akurasinya sebesar 92.2% .

Dapat ditentukan nilai akurasi yang lebih tinggi dengan menggunakan nilai K yang memiliki MSE yang juga lebih tinggi yaitu K =4 dengan akurasi sebesar 95.7%. Pada metode ini nilai akurasi bisa berubah dengan mengubah nilai K.

B. *Perbandingan Hasil Akurasi*

Perbandingan nilai akurasi berdasarkan nilai K yang memiliki nilai MSE terendah(Tabel II) dan nilai K dengan MSE tertinggi (Tabel III).

TABEL II. Perbandingan nilai K dengan MSE terendah

Perbandingan	
Nilai K	**Akurasi**
21	92.2%
19	92.3%
34	92.4%
11	92.5%
17	92.7%

TABEL III. Perbandingan nilai K dengan MSE tertinggi

Perbandingan	
Nilai K	Akurasi
4	95.7%
2	95.3%
5	94.7%
6	94.6%
1	94.55%

Dari tabel di atas (Tabel 2) diurutkan lima nilai K dengan MSE terendah. Nilai K disusun berdasarkan nilai MSE terendah ke nilai MSE tertinggi menghasilkan nilai akurasi yang juga berbeda. Dapat dilihat perbedaan nilai akurasi pada tabel 2 sangat kecil dengan kisaran 0.1% sampai dengan 0.2% walau perbandingan nilai akurasi pada tabel di atas sangat kecil namun hal itu cukup berpengaruh terhadap kestabilan hasil klasifikasi.

Pada tabel selanjutnya (Tabel 3) di urutkan nilai lima K dengan MSE tertinggi yang disusun dari nilai MSE tertinggi ke terendah. Dapat dilihat semakin tinggi nilai MSE semakin besar pula nilai akurasi yang di didapatkan. Perbandingan nilai akurasi dari lima nilai MSE tertinggi ini memiliki kisaran 0.05% sampai dengan 1.15%. Ternyata dapat dilihat perbandingan nilai akurasi dari lima nilai MSE tertinggi ini juga sangat kecil tetapi tidak sekecil perbandingan nilai MSE terendah.

IV. KESIMPULAN

Dari hasil dan pembahasan yang telah dilakukan dengan menggunakan metode KNN, kami mendapatkan hasil akurasi yang cukup tinggi, yaitu sebesar 92.2% dengan menggunakan K yang memiliki nilai MSE terendah, yaitu sebesar 21.

REFRENSI

[1] D. Ranganayakulu and C. Chellappan, "Detecting malicious URLs in E-mail--An implementation," *AASRI Procedia*, vol. 4, pp. 125–131, 2013.

[2] B. Eshete and V. N. Venkatakrishnan, "Webwinnow: Leveraging exploit kit workflows to detect malicious urls," in *Proceedings of the 4th ACM conference on Data and application security and privacy*, 2014, pp. 305–312.

[3] D. Canali, M. Cova, G. Vigna, and C. Kruegel, "Prophiler: a fast filter for the large-scale detection of malicious web pages," in *Proceedings of the 20th international conference on World wide web*, 2011, pp. 197–206.

ISBN : **978-979-587-813-1**
Vol.4 No.1

[4] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: learning to detect malicious web sites from suspicious URLs," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009, pp. 1245–1254.

[5] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Learning to detect malicious urls," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, p. 30, 2011.

[6] F. Liantoni, "Klasifikasi Daun Dengan Perbaikan Fitur Citra Menggunakan Metode K-Nearest Neighbor," *Ultim. Comput.*, vol. 7, no. 2, 2015.

[7] B. Hartono and V. Lusiana, "Pencarian Isi Citra Menggunakan Metode Minkowski Distance," *Proceeding SENDI_U*, 2017.

ISBN : 978-979-587-813-1
Vol.4 No.1