OPTIMALISASI TEKNIK KLASIFIKASI SERANGAN BOTNET DENGAN MENGGUNAKAN SELEKSI FITUR HASHMAP DAN K-NEAREST NEIGHBOR

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer

DISUSUN OLEH:

MUHAMMAD ILHAM NUARI

09011381924100

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

"OPTIMALISASI TEKNIK KLASIFIKASI SERANGAN BOTNET DENGAN MENGGUNAKAN SELEKSI FITUR HASHMAP DAN K-NEAREST NEIGHBOR"

PROPOSAL TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh :

Muhamad Ilham Nuari

09011381924100

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

Pembimbing

Ahmad Heryanto, S.Kom, M.T.

NIP. 198701222015041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 18 Juli 2023

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, S.Si., M.T**
2. **Sekretaris** : **Nurul Afifah, S.Kom., M.Kom**
3. **Penguji** : **Huda Ubaya, M.T**
4. **Pembimbing** : **Ahmad Heryanto, S.Kom., M.T**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

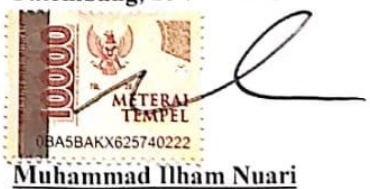
Nama	:	Muhammad Ilham Nuari
NIM	:	09011381924100
Judul	:	OPTIMALISASI TEKNIK KLASIFIKASI SERANGAN *BOTNET* DENGAN MENGGUNAKAN SELEKSI FITUR *HASHMAP* DAN *K-NEAREST NEIGHBOR*

Hasil Pengecekan Software Turnitin : 14%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, 18 Juli 2023



Muhammad Ilham Nuari
NIM. 09011381924100

HALAMAN PERSEMBAHAN

“Awali segalanya dengat Niat, berdoa, Berusaha, dan Brtawakal”.

Penulis:

“Muhammad Ilham Nuari”

Skripsi ini saya persembahan untuk:

Orang tua saya tercinta Bpk.Danial dan Ibu.Enorita yang tidak pernah letih dalam mendidik saya hingga saat ini dan tiada hentinya juga dalam memberikan nasihat, semangat, dan selalu memotivasi saya untuk menjadi orang sukses dan dapat bermanfaat bagi banyak orang dan Seluruh keluarga besar serta teman seperjuangan yang selalu memberi dukungan dan semangat.

Motto hidup
“Lebih dari 50% keberhasilan dari doa ibu”

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيْم

Assalamu'alaikum Warahmatullahi Wabarakatuh

Marilah kita panjatkan puji serta syukur atas kehadirat Allah SWT karena atas berkat hidayah dan karunia – Nya penulis dapat menyelesaikan penyusunan tugas akhir ini yang berjudul **"OPTIMALISASI TEKNIK KLASIFIKASI SERANGAN BOTNET DENGAN MENGGUNAKAN SELEKSI FITUR HASHMAP DAN K-NEAREST NEIGHBOR"**

Sebelumnya, penulis ingin memberikan serta mengucapkan terima kasih kepada beberapa pihak yang senantiasa memberikan ide, masukan, kritik, serta motivasi selama penulis melakukan penyusunan Tugas Akhir. Ucapan terima kasih tersebut ingin penulis sampaikan kepada :

1. Allah SWT yang senantiasa telah memberikan rahmat, hidayah serta karunia – Nya sehingga penulis bisa menyelesaikan penulisan Tugas Akhir ini.
2. Orang tua saya tercinta Bpk.Danial dan Ibu.Enorita yang tidak pernah letih dalam mendidik saya hingga saat ini dan tiada hentinya juga dalam memberikan nasihat, semangat, dan selalu memotivasi saya untuk menjadi orang sukses dan dapat bermanfaat bagi banyak orang.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si selaku PAW Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing yang telah berkenan meluangkan waktu dan tenaga dalam membimbing, memberikan saran serta memberikan motivasi kepada penulis selama proses penulisan Tugas Akhir ini.
6. Bapak Aditya Putra Perdana P, S.Kom., M.T. selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer penulis saat ini.

7. Kakak tingkat saya Agung Al Hafizin dan M.Robby Bahari yang telah memberikan berbagai bantuan selama penulis menjalani masa perkuliahan hingga akhir.
8. Mbak Sari Nuzulastri dan Mbak Renny Virgasari selaku admin jurusan sistem komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
9. Semua pihak yang terlibat yang telah turut ikut membantu, baik itu dalam memberikan masukan dan ide, kritik, maupun juga memberikan semangat kepada penulis yang mana tidak bisa disebutkan satu persatu.

Penulis menyadari bahwasanya penyusunan Tugas Akhir yang telah diselesaikan tidak mendekati kata sempurna. Maka dari itu penulis meminta kritik, masukan, serta ide yang dapat digunakan oleh penulis agar penyusunan Tugas Akhir dapat menjadi jauh lebih baik lagi di masa mendatang.

Palembang, 18 Juli 2023

Penulis,

Muhammad Ilham Nuari

NIM.09011381924100

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Muhammad Ilham Nuari (09011381924100)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : ajoilham120@gmail.com

ABSTRAK

Botnet terdiri dari sekelompok program perangkat lunak yang saling berhubungan yang berkomunikasi satu sama lain melalui internet untuk menjalankan fungsi yang ditunjuk. Perangkat lunak ini diprogram untuk beroperasi secara otomatis dalam jaringan. Driver botnet, juga dikenal sebagai master bot, mengontrol setiap komputer yang merupakan bagian dari jaringan botnet dari jarak jauh. Oleh karena itu, dapat disimpulkan bahwa jika komputer terinfeksi botnet, setelah terhubung ke jaringan, ia akan menjalankan perintah yang dikeluarkan oleh master bot. K-Nearest Neighbor (K-NN) adalah metode klasifikasi yang menggunakan mayoritas kategori pada K-NN untuk menentukan kategori dari data baru atau data testing. Dalam K-NN, k objek terdekat (mirip) dengan objek data baru dicari dalam data pelatihan. Hasil Pada Confusion Matrix Algoritma 50:50 Akurasi Presisi Recall F1-Score KNN 99,80% 99,77% 99,84% 99,80%. Hasil nilai rata-rata pada fitur seleksi hashmap menggunakan metode KNN dengan nilai akurasi 99,80%. Selanjutnya hasil dan analisa dari skenario yang digunakan pada ROC curve Algoritma Hashmap TPR FPR KNN 99,75% 0,27%. Hasil nilai rata-rata pada ROC curve menggunakan fitur seleksi hashmap menggunakan metode KNN dengan nilai TPR 99,75% Hasil dan analisa dari skenario yang digunakan pada fitur seleksi hashmap yang digunakan dengan confusion matrix Hasil Pada Confusion Matrix Algoritma 70:30 Akurasi Presisi Recall F1-Score KNN 99,71% 99,67% 99,75% 99,71%. Hasil nilai rata-rata pada fitur seleksi hashmap menggunakan metode KNN dengan nilai 99.71% Selanjutnya hasil dan analisa dari skenario yang digunakan pada ROC pada Algoritma Hashmap TPR FPR KNN 99,75% 0,32%. Hasil nilai rata-rata pada ROC curve menggunakan fitur seleksi hasmap menggunakan metode KNN dengan nilai TPR 99,75%. Hasil Pada Confusion Matrix Algoritma 90:10 Akurasi Presisi Recall F1-Score KNN 99,79% 99,75% 99,83% 99,79% . Hasil dari visualisasi parallel koordinat antara data benign dan botnet untuk pola warna biru menunjukkan binign dan warna hijau menggunakan Hashmap untuk melakukan seleksi fitur dimana terdapat 52 fitur, semakin sedikit fitur yang di gunakan maka training semakin cepat dan fitur yang telah di pilih merupakan fitur yang relavan .

Kata Kunci : *Botnet Attack, K-Nearest Neighbord, Hashmap, ROC*

Mengetahui,

Ketua Jurusan Sistem Komputer,	**Pembimbing Tugas Akhir,**
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom, M.T.**
NIP. 196612032006041001 NIP.	**NIP. 198701222015041002**

Optimization of Botnet Attack Classification Techniques Using Hashmap Feature Selection and K-Nearest Neighbord

Muhammad Ilham Nuari (09011381924100)
Computer Engineering Department, Computer Science Faculty, Sriwijaya University
Email : ajoilham120@gmail.com

ABSTRACT

A botnet consists of a group of interconnected software programs that communicate with each other via the internet to perform designated functions. This software is programmed to operate automatically in the network. A botnet driver, also known as a bot master, remotely controls each computer that is part of a botnet network. Therefore, it can be concluded that if a computer is infected with a botnet, after connecting to the network, it will execute commands issued by the bot master. K-Nearest Neighbor (K-NN) is a classification method that uses the majority of categories in K-NN to determine the category of new data or data testing. In K-NN, k objects closest (similar) to the new data object are searched in the training data. Results on the Confusion Matrix Algorithm 50:50 Precision Accuracy Recall F1-Score KNN 99.80% 99.77% 99.84% 99.80%. The results of the average value on the hashmap selection feature use the KNN method with an accuracy value of 99.80%. Furthermore, the results and analysis of the scenarios used in the Hashmap Hashmap ROC curve TPR FPR KNN 99.75% 0.27%. The results of the average value on the ROC curve using the hashmap selection feature using the KNN method with a TPR value of 99.75% Results and analysis of the scenarios used in the hashmap selection feature used with the confusion matrix Results in the Confusion Matrix Algorithm 70:30 F1 Recall Precision Accuracy - KNN score 99.71% 99.67% 99.75% 99.71%. The average value of the hashmap selection feature uses the KNN method with a value of 99.71%. Furthermore, the results and analysis of the scenario used in the ROC on the TPR FPR KNN Hashmap Algorithm are 99.75% 0.32%. The results of the average value on the ROC curve using the hasmap selection feature using the KNN method with a TPR value of 99.75%. Results on the Confusion Matrix Algorithm 90:10 Precision Accuracy Recall F1-Score KNN 99.79% 99.75% 99.83% 99.79%. The results of visualization of parallel coordinates between benign and botnet data for blue patterns show binign and green colors using Hashmap to perform feature selection where there are 52 features, the fewer features used, the faster the training and the features that have been selected are relevant features .

Keywords : *Botnet Attack, K-Nearest Neighbord, Hashmap, ROC*

Acknowledged,

Head of Computer Systems Department,	**Supervisor,**
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom, M.T.**
NIP. 196612032006041001 NIP.	**NIP. 198701222015041002**

BAB I
PENDAHULUAN

1.1 Latar Belakang

Botnet terdiri dari sekelompok program perangkat lunak yang saling berhubungan yang berkomunikasi satu sama lain melalui internet untuk menjalankan fungsi yang ditunjuk. Perangkat lunak ini diprogram untuk beroperasi secara otomatis dalam jaringan. Driver botnet, juga dikenal sebagai master bot, mengontrol setiap komputer yang merupakan bagian dari jaringan botnet dari jarak jauh. Oleh karena itu, dapat disimpulkan bahwa jika komputer terinfeksi botnet, setelah terhubung ke jaringan, ia akan menjalankan perintah yang dikeluarkan oleh master bot [1].

Peralatan yang telah rusak secara efektif dengan perangkat lunak berbahaya botnet dikenali sebagai bot atau mayat hidup. *Undead* selanjutnya dapat dimanfaatkan oleh bot-herder untuk merusak peralatan lain. Selanjutnya, perangkat lunak berbahaya menyebar sendiri secara otomatis ketika menemukan peralatan yang rentan. Dengan cara ini, dapat meningkatkan jumlah peralatan yang terkontaminasi oleh perangkat lunak berbahaya [2].

Jika jaringan robot telah merilis jumlah besar, bot-master akan menghubungkan semua perangkat yang terkontaminasi melalui jaringan yang dapat dikendalikan dari jarak jauh. Selanjutnya, bot-master akan memulai operasinya dengan menggunakan jaringan robot. Robot menyerang dengan mengeksploitasi kelemahan perangkat lunak dan menanamkan trojan seperti metode rekayasa sosial untuk mengambil kode robot jahat. Namun demikian, di tengah kategori lain dari perangkat lunak berbahaya, atribut yang menentukan dari jaringan robot adalah pemanfaatan saluran Command & Control (C & C) yang dapat dimodifikasi dan dialihkan. Saluran C&C yang memiliki struktur multi-tier. Jaringan robot menawarkan kenyamanan bagi bot-controller. Saluran C & C dapat berfungsi di wilayah topologi jaringan konseptual dan memanfaatkan beragam protokol komunikasi. Jaringan robot biasanya dikategorikan berdasarkan arsitektur perintah dan control [3].

Konsekuensi dari botnet yang menginfeksi perangkat adalah penurunan kinerja jaringan yang signifikan, melemahnya kecepatan internet, dan penurunan kinerja perangkat / komputer. Botnet juga mengkonsumsi sejumlah besar bandwidth dengan mengunduh informasi yang dibutuhkannya, dan pada akhirnya, ia dapat melumpuhkan sistem komputer, membuatnya tidak dapat dioperasikan [4].

Penelitian ini melibatkan beberapa teknik untuk mengidentifikasi malware bot, salah satunya adalah deteksi berbasis anomali. Binkley et.al (2012) mengusulkan perangkat yang menggabungkan data IRC dan TCP untuk menemukan botnet menggunakan deteksi total berbasis anomali. Demikian pula, Karasaridis et.al (2007) mengembangkan seperangkat aturan untuk analisis anomali berbasis pasif yang dapat menemukan pengontrol IRC botnet yang berjalan pada port acak tanpa tanda tangan yang dianggap atau kode biner umum. Tahap ini menggunakan teknik deteksi total berbasis anomali untuk deteksi botnet. Deteksi total berbasis anomali didasarkan pada pengunjung komunitas untuk menemukan anomali yang mencakup latensi komunitas yang berlebihan, volume lalu lintas yang berlebihan, lalu lintas port yang tidak biasa, dan perilaku perangkat yang tidak biasa yang akan menyiratkan adanya bot berbahaya di komunitas. Deteksi total berbasis anomali dibagi menjadi beberapa teknik, khususnya pendekatan total berbasis host dan pendekatan total berbasis komunitas[5].

Teknik yang dikenal sebagai pemantauan berbasis host digunakan untuk meneliti dan mengevaluasi komponen internal sistem komputer alih-alih berfokus pada antarmuka eksternal dan lalu lintas jaringan. Di sisi lain, deteksi berbasis jaringan adalah teknik yang bertujuan untuk mengidentifikasi botnet dengan mengawasi lalu lintas jaringan. Teknik khusus ini dapat diklasifikasikan menjadi dua jenis, yaitu pemantauan aktif dan pasif. Pemantauan aktif melibatkan penyuntikan paket uji ke server atau jaringan aplikasi untuk mengukur responsnya, tetapi dapat mengakibatkan lalu lintas tambahan di jaringan. Pemantauan jaringan pasif, di sisi lain, melibatkan penggunaan berbagai perangkat untuk mengamati aliran lalu lintas jaringan tanpa meningkatkan lalu lintas jaringan selama inspeksi. Teknik ini membutuhkan banyak waktu untuk mengamati berbagai tahap komunikasi dan aktivitas botnet untuk mendeteksi botnet. Investigasi sebelumnya tentang subjek deteksi botnet termasuk tesis Pedro Marques da Luz (2013-2014)

berjudul Botnet Detection Using Passive DNS (Domain Name System). Penyelidikan lain dilakukan oleh Septian Gegas pada tahun 2013, yang disebut Identifikasi Botnet Melalui Pemantauan Aktivitas Kelompok pada Lalu Lintas DNS (Domain Name System), yang bertujuan untuk mendeteksi botnet dengan mengamati aktivitas kelompok dalam Permintaan DNS. Perbedaan dalam diskusi yang disajikan terletak pada penggunaan DNS (Domain Name System) yang berbeda dan teknik alternatif dari penelitian sebelumnya. Secara khusus, penelitian ini menggunakan metode K-NN untuk menguji DNS (Domain Name System) yang diekstraksi dari dataset CTU-13 dan dievaluasi melalui K-Fold Cross Validation and Compusion Metric [6].

Untuk membedakan antara serangan botnet dan jenis serangan lainnya, para ahli mengandalkan metode K-Nearest Neighbor (K-NN). Keuntungan dari metode ini sangat banyak, dapat secara efektif menangani data yang bising, sangat cocok untuk kumpulan data besar, dan relatif mudah diterapkan. Namun, ada juga beberapa kelemahan untuk menggunakan metode K-NN, seperti kebutuhan untuk menentukan nilai parameter, sensitivitas terhadap data pencilan, dan kerentanan terhadap variabel non-informatif [7]

Disediakan dalam penggambaran di atas, para sarjana dapat memperoleh rincian tentang cara meningkatkan dan mengkategorikan Serangan Botnet dengan memanfaatkan teknik K-NN. Pendekatan K-NN mampu mengklasifikasikan entitas dengan belajar dari data yang paling mirip dengan entitas. Tujuannya adalah untuk mengklasifikasikan entitas baru berdasarkan karakteristik dan kereta sampel. Selanjutnya, peneliti memanfaatkan fungsi HashMap[8].

HashMap adalah koleksi Java yang memfasilitasi organisasi dan penyajian data. Ini berfungsi seperti array asosiatif di Java [9]. Memanfaatkan kemampuan pemilihan fitur HashMap, seseorang dapat memperoleh fitur yang paling sesuai dari seluruh dataset. Tujuan dari pilihan karakteristik adalah untuk memilih bagian dari area karakteristik awal yang lebih informatif untuk keindahan tujuan dalam pelaksanaan tugas pembelajaran perangkat, sementara mengabaikan di samping titik dan fitur yang berlebihan. Informasi di dalam Fitur Opsi HashMap dikompilasi menggunakan pasangan kunci-harga.

Berdasarkan latar belakang masalah uraian diatas, penulis tertarik memilih judul penelitian yaitu **"Optimalisasi Tekhnik Klasifikasi Serangan Botnet dengan Menggunakan Seleksi Fitur Hashmap dan K-Nearest Neighbor".**

1.2 Perumusan dan Batasan Masalah

1.2.1 Perumusan Masalah

Berkenaan identifikasi masalah diatas maka penulis mencoba merumuskan masalah yang akan dibahas dalam penelitian ini yaitu :

1. Bagaimana serangan *Botnet* terjadi pada jaringan atau komputer ?
2. Bagaimana cara mencegah agar dapat terhindar dari serangan *Botnet*?
3. Bagaimana penerapan model metode KNN dapat menangani klasifikasi serangan botnet pada data set CIC-IDS -2018

1.2.2 Batasan Masalah

Berkenaan identifikasi masalah diatas maka penulis mencoba merumuskan masalah yang akan dibahas dalam penelitian ini yaitu :

1. Penelitian ini menggunakan metode *K-Nearest Neighbor* (K-NN) untuk mendeteksi serangan.
2. Penelitian menggunakan dataset dari CIC-IDS 2018.
3. Output yang dihasilkan dari penelitian ini berupa optimaliasasi serangan *Botnet* menggunakan Metode *K-Nearest Neighbor* (K-NN) serta solusi alternatif dalam pencegahannya.
4. Algoritma implementasi yang di gunakan dalam penelitian adalah Algoritma *K-Nearest Neighbor* (K-NN).

1.3 Tujuan dan Manfaat

1.3.1 Tujuan

Berdasarkan identifikasi masalah dan atasan diatas, tujuan dari penelitian ini adalah sebagai berikut :

1. Mendeteksi serangan Botnet dengan menggunakan metode *K-Nearest Neighbord* (K-NN).
2. Membuat Analisa sebagai solusi atas dampak dalam mencegah serangan Botnet.

3. Menerapkan Algoritma K-NN dengan pendeteksian serangan Botnet pada data set CIC-IDS 2018.

1.3.2 Manfaat

Berdasarkan identifikasi masalah, batasan, serta tujuan diatas dari penelitian ini maka penelitian ini terdapat manfaat sebagai berikut :

1. Optimalisasi serangan *botnet* dengan menggunakan metode K-NN dapat memberikan hasil akurasi yang optimal.
2. Memberikan informasi mengenai metode K-NN dan pengaplikasian dalam serangan *botnet.*
3. Memberikan infromasi mengenai data set Botnet yang digunakan dalam penelitian.

1.4 . Metode Penelitian

1.4.1. Sistematika Penelitian

Komposisi dokumen tugas penutup disusun menjadi sejumlah bagian bawahan yang akan diuraikan secara luas, merinci metodologi penelitian penulis. Tujuan dari dokumen ini adalah untuk secara sistematis menyajikan ikhtisar topik yang akan dibahas. Struktur dokumen ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Bab I membawa latar belakang, ke formula kerumitan dan tujuan dan manfaat, di samping sistematika penulisan di dalam proyek terakhir.

BAB II. TINJAUAN PUSTAKA

Bab II membawa evaluasi literatur yang membawa landasan teoritis di dalam dialog studi ini dan kerangka teoritis.

BAB III. METEDOLOGI PENELITIAN

Bab III memuat catatan tentang pengumpulan statistik, spesifikasi perangkat keras dan perangkat lunak yang digunakan, selain teknik dan diagram alur yang digunakan dalam penelitian

BAB IV. PEMBAHASAN

Bab IV menggabungkan dialog pusat studi yang telah selesai dan tambahan menggabungkan evaluasi efek dari studi.

BAB V. KESIMPULAN DAN SARAN

Bab V mencakup kesimpulan dari bab-bab yang telah diberikan terutama berdasarkan hasil mengoptimalkan strategi kategori serangan botnet, penggunaan opsi karakteristik hashmap dan K-Nearest Neighbord (K-NN), dan kebangkrutan ini terdiri dari rekomendasi yang dapat diprediksi bermanfaat untuk penelitian di masa depan.

Daftar Pustaka

[1] A. Nugraha and F. A. Rafrastara, "Botnet Detection Survey," *Semin. Nas. Teknol. Inf. Komun. Terap. 2011*, vol. 1, no. Semantik, 2011.

[2] R. F. M. Dollah, M. A. Faizal, F. Arif, M. Z. Mas'ud, and L. K. Xin, "Machine learning for HTTP botnet detection using classifier algorithms," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, no. 1–7, pp. 27–30, 2018.

[3] M. Farizi, "Pengelompokan Spam Botnet Dengan Metode Fuzzy Hashing," *J. Telemat. MKOM Vol*, vol. 12, no. 1, 2020, [Online]. Available: https://www.academia.edu/download/65315706/telematikamkom_v12n1.pdf

[4] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced Support Vector Machine-(ASVM-) based detection for Distributed Denial of Service (DDoS) attack on Software Defined Networking (SDN)," *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/8012568.

[5] I. Syamsuddin and O. M. Barukab, "SUKRY : Suricata IDS with Enhanced kNN Algorithm on," *Electronics*, vol. 11, no. 737, 2022.

[6] M. S. Rafsanjani, F. Informatika, U. Telkom, and R. Forest, "Deteksi Serangan Botnet Pada Jaringan Internet of Things Menggunakan Algoritma Random Forest (RF)," vol. 9, no. 3, pp. 1862–1871, 2022.

[7] J. Pseudocode, V. I. I. I. Nomor, S. Kasus, D. Pemuda, and P. Bengkulu, "127887-ID-implementasi-metode-k-nearest-neighbor-k," vol. III, no. 0065, pp. 98–112, 2021.

[8] D. Gunawan, T. Hairani, and A. Hizriadi, "Botnet identification based on flow traffic by using K-nearest neighbor," *2019 Int. Conf. Adv. Comput. Sci. Inf. Syst. ICACSIS 2019*, pp. 95–100, 2019, doi: 10.1109/ICACSIS47736.2019.8979738.

[9] A. Niranjan, K. M. Akshobhya, P. D. Shenoy, and K. R. Venugopal, "EKNIS: Ensemble of KNN, Naïve Bayes Kernel and ID3 for Efficient Botnet Classification Using Stacking," *2018 Int. Conf. Data Sci. Eng. ICDSE 2018*, no. August, pp. 1–6, 2018, doi: 10.1109/ICDSE.2018.8527791.

[10] T. Suryana, "Mengenal HashMap dalam Pemrograman Java," 2021.

[11] R. Hadianto and T. W. Purboyo, "A simulation study of SDN defense against Botnet attack based on network traffic detection," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 10, pp. 3489–3494, 2018.

[12] I. Ali *et al.*, "Systematic Literature Review on IoT-Based Botnet Attack," *IEEE Access*, vol. 8, pp. 212220–212232, 2020, doi: 10.1109/ACCESS.2020.3039985.

[13] F. Hussain *et al.*, "A Two-Fold Machine Learning Approach to Prevent and

Detect IoT Botnet Attacks," *IEEE Access*, vol. 9, pp. 163412–163430, 2021, doi: 10.1109/ACCESS.2021.3131014.

[14] S. Dhanabal and S. Chandramathi, "A Review of various k-Nearest Neighbor Query Processing Techniques," *Int. J. Comput. Appl.*, vol. 31, no. 7, pp. 14–22, 2011, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:A+Review+of+various+k-Nearest+Neighbor+Query+Processing+Techniques#0

[15] A. Kataria and M. D. Singh, "A Review of Data Classification Using K-Nearest Neighbour Algorithm," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 6, pp. 354–360, 2013.

[16] S. B. Imandoust and M. Bolandraftar, "Application of K-Nearest Neighbor (KNN) Approach for Predicting Economic Events : Theoretical Background," *Int. J. Eng. Res. Appl.*, vol. 3, no. 5, pp. 605–610, 2013.

[17] Irfan, I. M. Wildani, and I. N. Yulita, "Classifying Botnet Attack on Internet of Things Device Using Random Forest," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 248, no. 1, 2019, doi: 10.1088/1755-1315/248/1/012002.

[18] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," *Sensors (Switzerland)*, vol. 20, no. 16, pp. 1–15, 2020, doi: 10.3390/s20164372.

[19] A. M. Almuhaideb and D. Y. Alynanbaawi, "Applications of Artificial Intelligence to Detect Android Botnets: A Survey," *IEEE Access*, vol. 10, no. April, pp. 71737–71748, 2022, doi: 10.1109/ACCESS.2022.3187094.

[20] M. Yusof, M. M. Saudi, and F. Ridzuan, "A new mobile botnet classification based on permission and API calls," *Proc. - 2017 7th Int. Conf. Emerg. Secur. Technol. EST 2017*, no. September, pp. 122–127, 2017, doi: 10.1109/EST.2017.8090410.

[21] K. Huang, L. X. Yang, X. Yang, Y. Xiang, and Y. Y. Tang, "A Low-Cost Distributed Denial-of-Service Attack Architecture," *IEEE Access*, vol. 8, pp. 42111–42119, 2020, doi: 10.1109/ACCESS.2020.2977112.

[22] B. I. Hairab, M. Said Elsayed, A. D. Jurcut, and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," *IEEE Access*, vol. 10, no. September, pp. 98427–98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[23] A. Mahboubi, S. Camtepe, and K. Ansari, "Stochastic modeling of IoT Botnet spread: A short survey on mobile malware spread modeling," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3044277.

[24] R. H. Randhawa, N. Aslam, M. Alauthman, H. Rafiq, and F. Comeau, "Security Hardening of Botnet Detectors Using Generative Adversarial Networks," *IEEE Access*, vol. 9, pp. 78276–78292, 2021, doi: 10.1109/ACCESS.2021.3083421.

[25] M. Panda, A. A. A. Mousa, and A. E. Hassanien, “Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks,” *IEEE Access*, vol. 9, pp. 91038–91052, 2021, doi: 10.1109/ACCESS.2021.3092054.

[26] R. Kalakoti, S. Nomm, and H. Bahsi, “In-Depth Feature Selection for the Statistical Machine Learning-Based Botnet Detection in IoT Networks,” *IEEE Access*, vol. 10, no. July, pp. 94518–94535, 2022, doi: 10.1109/ACCESS.2022.3204001.

[27] M. Reza Noviansyah, T. Rismawan, D. Marisa Midyanti, J. Sistem Komputer, and F. H. MIPA Universitas Tanjungpura Jl Hadari Nawawi, “Penerapan Data Mining Menggunakan Metode K-Nearest Neighbor Untuk Klasifikasi Indeks Cuaca Kebakaran Berdasarkan Data Aws (Automatic Weather Station) (Studi Kasus: Kabupaten Kubu Raya),” *J. Coding, Sist. Komput. Untan*, vol. 06, no. 2, pp. 48–56, 2018.

[28] B. M. Randles, I. V. Pasquetto, M. S. Golshan, and C. L. Borgman, “Using the Jupyter Notebook as a Tool for Open Science: An Empirical Study,” *Proc. ACM/IEEE Jt. Conf. Digit. Libr.*, 2017, doi: 10.1109/JCDL.2017.7991618.

[29] T. Kluyver *et al.*, “Jupyter Notebooks—a publishing format for reproducible computational workflows,” *Position. Power Acad. Publ. Play. Agents Agendas - Proc. 20th Int. Conf. Electron. Publ. ELPUB 2016*, pp. 87–90, 2016, doi: 10.3233/978-1-61499-649-1-87.

[30] J. Wang, T. Y. Kuo, L. Li, and A. Zeller, “Assessing and Restoring Reproducibility of Jupyter Notebooks,” *Proc. - 2020 35th IEEE/ACM Int. Conf. Autom. Softw. Eng. ASE 2020*, pp. 138–149, 2020, doi: 10.1145/3324884.3416585.