OPTIMALISASI MODEL DETEKSI SERANGAN *SMURF DDOS* PADA *SOFTWARE DEFINED NETWORK* MENGGUNAKAN METODE *DECISION TREE* DAN *K-NEAREST NEIGHBOR*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

DISUSUN OLEH :

AL MAIS

09011381823107

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

OPTIMALISASI MODEL DETEKSI SERANGAN *SMURF DDOS* PADA *SOFTWARE DEFINED NETWORK* MENGGUNAKAN METODE ALGORITMA *DECISION TREE* DAN *K-NEAREST NEIGHBOR*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Jenjang S-1

Oleh :

AL MAIS
09011381823107

Palembang, Desember 2022

Pembimbing Tugas Akhir I	Pembimbing Tugas Akhir II
Ahmad Heryanto, S. Kom, M.T	**Tri Wanda Septian, M.Sc**
NIP. 198701222015041002	**NIK. 1901062809890001**

Mengetahui, 16/12/22

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Rabu**

Tanggal : **07 Desember 2022**

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, M.T.** (.....)
2. **Sekretaris** : **Aditya Putra Perdana P, M.T.** (.....)
3. **Pembimbing I** : **Ahmad Heryanto, M.T.** (.....)
4. **Pembimbing II** : **Tri Wanda Septian, M. Sc.** (.....)
5. **Penguji** : **Kemahyanto Exaudi, M.T.** (.....)

Mengetahui, 22/12/22

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Al Mais

NIM : 09011381823107

Judul : Optimalisasi Model Deteksi Serangan Smurf DDoS Pada Software Defined Network Menggunakan Metode Decision Tree Dan K-Nearest Neighbor

Hasil Pengecekan Software iThenticate/Turnitin : 12%

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

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, 07 Desember 2022

Al Mais
NIM. 09011381823107

HALAMAN PERSEMBAHAN

“Sesungguhnya bersama kesulitan itu ada kemudahan, maka apabila engkau telah selesai (dari suatu urusan), tetaplah bekerja keras (untuk urusan yang lain), dan hanya kepada Tuhanmulah engkau berharap.”

(Q.S. Al Insyirah Ayat 6-8)

Tugas Akhir ini kupersembahkan untuk :

Kedua Orang Tua Saya

(Isnadi dan Ardilah)

Keluarga Besarku

(Kakak-kakakku)

Teman-Teman Seperjuanganku

(Sistem Komputer 2018)

Almamaterku

(Universitas Sriwijaya)

Dan semua pihak yang bertanya :

“Kapan sidang?”, “Kapan nyusul?”, “Kapan lulus?” dan sebagainya.

Kalian semua adalah alasanku untuk segera menyelesaikan tugas akhir ini.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيْم

Assalamualaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas kehadirat Allah SWT Tuhan Yang Maha Esa, yang atas segala berkat, kasih sayang, serta karunia-Nya penulis dapat menyelesaikan penulisan proposal tugas akhir ini yang berjudul "**Optimalisasi Model Deteksi Serangan *Smurf* DDOS Pada *Software Defined Network* Menggunakan Metode Algoritma *Decision Tree* Dan *K-Nearest Neighbor***".

Pada penyusunan laporan ini, penulis ingin mengucapkan terima kasih karena banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan berterima kasih kepada :

1. Allah SWT yang senantiasa memberikan rahmat dan karunia-Nya sehingga saya bisa menyelesaikan tugas akhir ini.
2. Kedua orang tua, saudara, dan keluarga besar yang tiada hentinya selalu mendoakan dan memberikan motivasi dan dukungan yang terbaik hingga bisa menyelesaikan tugas akhir ini dengan baik dan lancar.
3. Bapak Jaidan Jauhari, S.Pd, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer sekaligus Dosen Pembimbing Akademik Jurusan Sistem Komputer.
5. Bapak Ahmad Heryanto, S. Kom, M.T. selaku Dosen Pembimbing I Tugas Akhir dan Bapak Tri Wanda Septian, M.Sc. selaku Dosen Pembimbing II Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.

6. Mbak Sari selaku Admin Jurusan Sistem Komputer Unggulan yang telah membantu melancarkan proses sidang akhir dan urusan administrasi terkait tugas akhir saya.
7. Rizky Angga Pratama dan M. Alfat Hayatur Rizon selaku asisten lab jaringan komputer kampus bukit yang telah meminjamkan fasilitas lab semasa pengerjaan tugas akhir.
8. M. Rifqi Abiyyu Ariq, Christoper Marlo, M. Dion Iqbal, teman-teman dari SK 19 dan semua teman-teman asisten lab comnet lantai 5 kampus bukit yang telah menemani dan meminjamkan fasilitas semasa pengerjaan tugas akhir.
9. Jarkom gang yang telah membantu serta membersamai dalam mengerjakan dan saling membantu dalam proses pengerjaan tugas akhir.
10. Teman-teman seperjuangan yang lainnya yang selalu menghibur, memberi motivasi dan menemani dari awal hingga akhir perkuliahan.
11. Seluruh staff dan pegawai Jurusan Sistem Komputer dan semua pihak yang telah membantu yang tidak bisa disebutkan satu persatu.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Kritik dan saran yang diberikan sangatlah diharapkan penulis agar dapat segera memperbaiki laporan ini hingga dapat dijadikan sebagai masukkan ide yang bermanfaat bagi semua pihak yang dapat berguna untuk di masa yang akan mendatang.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, Desember 2022

Penulis,

Al Mais
NIM. 09011381823107

OPTIMIZATION OF SMURF DDOS ATTACK DETECTION MODEL IN SOFTWARE DEFINED NETWORK USING DECISION TREE AND K-NEAREST NEIGHBOR

Al Mais (09011381823107)

Dept. Of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Email : mais2820@gmail.com

ABSTRACT

This study focuses on the dataset from DDoS Attack SDN Dataset (2020) where the Smurf DDoS attack focuses on the ICMP protocol. The purpose of this study is to detect Smurf DDoS attacks on the Software Defined Network topology and analyze the accuracy and performance as well as compare two machine learning methods used. The method used in this study is the Decision Tree and K-Nearest Neighbor and Pearson Correlation as a feature selection in the dataset. The results of this study indicate that the Decision Tree has a better accuracy and performance value of 97.05% compared to the K-Nearest Neighbor value of 93.42% by using a dataset that has gone through a feature selection process. The parameter values used in each method also greatly affect the resulting accuracy and performance values in detecting Smurf DDoS attacks on the network.

Keywords : *Software Defined Network*, *Smurf DDoS*, *K-Nearest Neighbor*, *Decision Tree*

Palembang, December 07th 2022

Supervisor I	**Supervisor II**
Ahmad Heryanto, S. Kom, M.T	**Tri Wanda Septian, M.Sc**
NIP. 198701222015041002	**NIK. 1901062809890001**

Acknownledged,

Head of Computer Systems Department

Dr.Ir. H. Sukemi, M.T.

NIP. 196612032006041001

OPTIMALISASI MODEL DETEKSI SERANGAN *SMURF DDOS* PADA *SOFTWARE DEFINED NETWORK* MENGGUNAKAN METODE *DECISION TREE* DAN *K-NEAREST NEIGHBOR*

Al Mais (09011381823107)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : mais2820@gmail.com

ABSTRAK

Penelitian ini berfokus pada dataset dari *DDoS Attack SDN Dataset* (2020) dimana serangan *Smurf DDoS* berfokus pada protokol ICMP. Tujuan dari penelitian ini adalah mendeteksi serangan *Smurf DDoS* pada topologi *Software Defined Network* dan menganalisis akurasi dan performa serta membandingkan kedua metode *machine learning* yang digunakan. Metode yang digunakan dalam penelitian ini adalah *Decision Tree* dan *K-Nearest Neighbor* serta *Pearson Correlation* sebagai fitur seleksi pada dataset. Hasil dari penelitian ini menunjukkan bahwa metode *Decision Tree* memiliki nilai akurasi dan performa yang lebih baik sebesar 97.05% dibandingkan metode *K-Nearest Neighbor* sebesar 93.42% dengan menggunakan dataset yang telah melalui proses fitur seleksi. Nilai parameter yang digunakan pada tiap metode juga sangat berpengaruh terhadap nilai akurasi dan performa yang dihasilkan dalam mendeteksi serangan *Smurf DDoS* pada jaringan.

Kata Kunci : *Software Defined Network*, *Smurf DDoS*, *K-Nearest Neighbor*, *Decision Tree*

Palembang, 07 Desember 2022

Pembimbing Tugas Akhir I	**Pembimbing Tugas Akhir II**
Ahmad Heryanto, S. Kom, M.T	**Tri Wanda Septian, M.Sc**
NIP. 198701222015041002	**NIK. 1901062809890001**

Mengetahui, 16/12/22
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Software Defined Network (SDN) adalah pendekatan yang digunakan untuk merancang arsitektur jaringan komputer yang dinamis dan mudah diatur. Oleh karena itu, SDN diimplementasikan di banyak topologi untuk menawarkan konfigurasi yang lebih efisien, kinerja yang lebih baik, dan fleksibilitas yang lebih tinggi untuk memfasilitasi desain jaringan yang baru [1]. Namun, sama seperti konsep jaringan pada umumnya, *SDN* juga menghadapi berbagai ancaman dari banyaknya serangan jaringan. Jenis serangan yang umum terjadi pada teknologi jaringan adalah serangan *DDoS*. [2]. Serangan *DDoS* dapat mengakibatkan kerusakan pada perangkat jaringan dan mengganggu lalu lintas jaringan pada *SDN controller* atau terkadang juga membuat jaringan tidak tersedia. Serangan *DDoS* sangat mempengaruhi sistem dan juga mengganggu pola aliran jaringan. Serangan *DDoS* dianggap sebagai salah satu ancaman utama tidak hanya untuk jaringan tetapi juga untuk internet serta menurunkan efisiensi jaringan secara keseluruhan. Serangan *DDoS* dapat mengakibatkan *flooding* sehingga menghambat lalu lintas dan menyulitkan paket untuk mengalir dan mengikuti rute yang benar. Agar aliran paket menjadi lancar di jaringan, serangan *DDoS* harus dikurangi. Banyak penelitian sebelumnya yang dilakukan untuk mendeteksi serangan *DDoS* ini mengunakan metode *Machine Learning*. Pendekatan *Machine Learning* dapat menentukan algoritma tertentu yang mencakup formulasi dalam menentukan parameter untuk menemukan pola dan rute paket yang diperlukan untuk membuat deteksi menjadi lebih mudah [3].

Dalam penelitian [4], peneliti membuat sistem deteksi menggunakan algortima *Decision Tree* dan mitigasi serangan *DDoS* dengan metode *drop packet* pada *Software Defined Network*. Peneliti menggunakan dataset CICIDS 2017 dan kemudian menjadi pendeteksi serangan *DDoS* jenis *User Data Protocol* (UDP). Peneliti berhasil membangun sistem deteksi dan mitigasi serangan *DDoS* yang dibuktikan dengan berbagai skenario pengujian.

Pembentukan model pendeteksian (*rule detection*) bergantung kepada dataset acuan, yang kemudian dilakukan proses *learning* untuk mendapatkan pola serangan dan dibentuk menjadi pohon keputusan untuk melabeli setiap paket yang masuk. Model pendeteksian dengan *Decision Tree* yang dibangun melalui proses *learning* mendapatkan akurasi sebesar 99.95% dan dibuktikan dengan simulasi serangan dan pengujian.

Dalam penelitian [5], mereka mengembangkan sistem deteksi *IDS* menggunakan metode *K-Nearest Neighbor* untuk mengklasifikasikan jenis serangan normal, *DOS* dan *Probing*. Tujuan dari penelitian ini adalah untuk memantau trafik pada jaringan dan menentukan apakah trafik tersebut aman atau terdapat serangan. Pada metode *K-Nearest Neighbor* nilai k menjadi komponen penting yang berpengaruh terhadap akurasi yang akan diklasifikasi. Pada penilitian ini digunakan rentang nilai k dari 3 sampai 9. Akurasi terbesar yang dicapai pada penelitian ini sebesar 90% pada saat jumlah *data training* 3000 dan nilai K=5. Namun secara umum dengan adanya penambahan nilai k dapat menyebabkan penurunan nilai akurasi.

Dalam penelitian [6], peneliti melakukan berbagai perbandingan terhadap beberapa jenis metode Deep Learning dalam mendeteksi serangan *DDoS* pada *SDN* seperti *CNN*, *LSTM*, dan *MLP*. Selama tahap pengujian, metode tersebut menggunakan dua skenario pengujian. Dalam skenario pertama, mereka mengevaluasi sistem yang diusulkan untuk mendeteksi serangan *UDP flood* di lingkungan jaringan *SDN* dengan tingkat transmisi tinggi. Lalu lintas jaringan dianalisis mendekati waktu nyata, yang dilakukan dalam interval waktu satu detik. Hasil yang diperoleh oleh sistem lebih baik daripada metode lain yang dibandingkan di lingkungan pengujian itu. Menurut metrik yang dievaluasi, sistem mampu mendeteksi dan bertahan terhadap *DDoS* yang dilakukan. Dalam skenario kedua, mereka menguji kinerja sistem untuk mendeteksi serangan *DDoS* terhadap aplikasi yang berbeda. Dalam skenario itu, metode yang dibandingkan kurang akurat dalam mendeteksi serangan ini.

Pada penelitian ini, penulis akan menggunakan metode *Decision Tree* dan *K-Nearest Neighbor* dalam membuat model klasifikasi serangan *Smurf DDoS*

pada *SDN*. Penelitian ini bertujuan untuk mengetahui seberapa besar tingkat akurasi dari model deteksi dengan menggunakan metode tersebut dalam mendeteksi serangan *DDoS*. Dataset yang digunakan dalam penelitian ini menggunakan dataset yang berasal dari *DDoS Attack SDN Dataset* [7]. Dengan melakukan penelitian ini, penulis diharapkan dapat membuat sebuah rancangan model deteksi yang memiliki tingkat akurasi lebih baik lagi untuk kedepannya.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu bagaimana membuat deteksi serangan menggunakan metode *Decision Tree* dan *K-Nearest Neighbor* pada serangan *Smurf DDoS*, serta bagaimana menentukan deteksi serangan yang lebih optimal dalam mendeteksi serangan jaringan *Smurf DDoS* ini.

1.3 Batasan Masalah

Batasan masalah dari tugas akhir ini, yaitu :

1. Penelitian ini menggunakan data serangan *DDoS SDN* yang berasal dari penelitian sebelumnya.
2. Metode yang digunakan untuk mendeteksi dan mengklasifikasikan serangan adalah *Decision Tree* dan *K-Nearest Neighbor*.
3. Dataset serangan *DDoS* ini dilakukan pada topologi *Software Defined Network*.

1.4 Tujuan

Tujuan dari penulisan tugas akhir ini yaitu :

1. Menerapkan dan menguji metode *K-Nearest Neighbor* dan *Decision Tree* dalam mengklasifikasi serangan *Smurf DDoS*.
2. Melakukan analisa dan perbandingan hasil akurasi terhadap deteksi yang digunakan dalam penelitian ini untuk mendapatkan hasil akurasi terbaik.

1.5 Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu :

1. Mengenali pola serangan *Smurf DDoS* pada *Software Defined Network*.

2. Memahami cara kerja dari metode *K-Nearest Neighbor* dan *Decision Tree* yang digunakan dalam mengklasifikasi serangan *Smurf DDoS*.

1.6 Metodologi Penelitian

1. Studi Pustaka dan Literatur

   Pada tahap pertama, penulis mencari suatu permasalahan untuk dibahas yang bisa diangkat sebagi sebuah penelitian. Penulis mencari beberapa sumber referensi seperti jurnal, buku, artikel dan lain-lainnya yang memiliki keterkaitan dengan tugas akhir ini.
2. Perancangan dan Pembuatan Model

   Tahap kedua ini akan membahas mengenai langkah-langkah dalam merancang model yang dibuat berdasarkan perumusan masalah penelitian. Pada tahap ini, penulis membangun dan menerapkan algoritma yang akan digunakan. Setelah itu penulis menentukan perangkat *hardware* dan *software* yang digunakan untuk membuat model deteksi serangan jaringan pada penelitian tugas akhir.
3. Pengujian

   Tahap ketiga ini membahas pengujian yang dilakukan berdasarkan metodologi penelitian yang telah ditentukan. Tahap ini bertujuan untuk mendapatkan hasil pengujian yang sesuai dengan konsep yang telah ditentukan.
4. Analisis

   Pada tahap keempat, penulis melakukan analisis data yang diperoleh dari hasil pengujian untuk mengetahui apa saja kelebihan dan kekurangan pada pengujian dengan menggunakan metode tersebut.
5. Kesimpulan

   Pada tahap kelima, penulis mendapatkan suatu kesimpulan dari hasil pengujian dan analisa sebelumnya, sehingga kesimpulan ini dapat dijadikan dikembangkan pada landasan penelitian selanjutnya.

1.7 Sistematika Penulisan

Untuk memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari tiap bab, maka dibuat suatu sistematika penulisan sebagai berikut :

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah dan Batasan Masalah serta Metodologi Penelitian dan Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitian yang terkait dengan Software Defined Network, Distributed Denial Of Service, Decision Tree dan K-Nearest Neighbour. Bab ini akan menjadi landasan teori terhadap penelitian yang dilakukan.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai bagaimana proses penelitian tersebut dilakukan. Penjelasan pada bab ini meliputi dataset, kebutuhan perangkat yang digunakan dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISIS

Bab ini menjelaskan mengenai hasil dari pengujian yang telah dilakukan dalam penelitian serta analisis dari tiap data yang diperoleh dari hasil pengujian.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan akhir tentang penelitian yang telah dilakukan, serta menjawab setiap tujuan yang hendak dicapai sesuai yang tercantum pada BAB I (Pendahuluan). Pada bab ini juga terdapat beberapa saran yang mungkin diperlukan oleh peneliti lain untuk melakukan pengembangan penelitian selanjutnya yang lebih baik lagi.

DAFTAR PUSTAKA

[1] S. Krishnan and E. Oliver John Joel, "Mitigating DDoS attacks in software defined networks," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, vol. 2019-April, no. Icoei, pp. 960–963, 2019, doi: 10.1109/icoei.2019.8862589.

[2] H. E. Wahanani, B. Nugroho, and G. I. Prakoso, "Analisa Serangan Smurf Dan Ping of Death Dengan Metode Support Vector Machine (Svm)," *Anal. Serangan Smurf Dan Ping Death Dengan Metod. Support Vector Mach. (Svm)*, 2016.

[3] G. Kaur and P. Gupta, "Hybrid Approach for detecting DDOS Attacks in Software Defined Networks," *2019 12th Int. Conf. Contemp. Comput. IC3 2019*, pp. 1–6, 2019, doi: 10.1109/IC3.2019.8844944.

[4] M. Q. Syahputra, D. R. Akbi, and D. Risqiwati, "Deteksi Dan Mitigasi Serangan DDoS Pada Software Defined Network Menggunakan Algoritma Decision Tree," *J. Repos.*, vol. 2, no. 11, p. 1491, 2020, doi: 10.22219/repositor.v2i11.795.

[5] Y. Ariyanto, V. Al, H. Firdaus, and H. Pramana, "Klasifikasi Jenis serangan DOS dan Probing pada IDS menggunakan metode K- Nearest Neighbor," vol. 3, pp. 1–5, 2020.

[6] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments," *Futur. Gener. Comput. Syst.*, vol. 125, pp. 156–167, 2021, doi: 10.1016/j.future.2021.06.047.

[7] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," *J. Netw. Comput. Appl.*, vol. 187, no. May, p. 103108, 2021, doi: 10.1016/j.jnca.2021.103108.

[8] A. V. Kachavimath, S. V. Nazare, and S. S. Akki, "Distributed Denial of

Service Attack Detection using Naïve Bayes and K-Nearest Neighbor for Network Forensics," *2nd Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2020 - Conf. Proc.*, no. Icimia, pp. 711–717, 2020, doi: 10.1109/ICIMIA48430.2020.9074929.

[9] G. F. Scaranti, L. F. Carvalho, S. Barbon, and M. L. Proenca, "Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-Defined Networks," *IEEE Access*, vol. 8, pp. 100172–100184, 2020, doi: 10.1109/ACCESS.2020.2997939.

[10] A. Maslan, K. M. Mohammad, F. Binti Mohd Foozy, and S. N. Rizki, "DDoS detection on network protocol using neural network with feature extract optimization," *Proc. ICAITI 2019 - 2nd Int. Conf. Appl. Inf. Technol. Innov. Explor. Futur. Technol. Appl. Inf. Technol. Innov.*, pp. 60–65, 2019, doi: 10.1109/ICAITI48442.2019.8982136.

[11] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[12] I. Ramadhan, P. Sukarno, and M. A. Nugroho, "Comparative Analysis of K-Nearest Neighbor and Decision Tree in Detecting Distributed Denial of Service," *2020 8th Int. Conf. Inf. Commun. Technol. ICoICT 2020*, pp. 16–19, 2020, doi: 10.1109/ICoICT49345.2020.9166380.

[13] H. Y. Chang, T. L. Lin, T. F. Hsu, Y. S. Shen, and G. R. Li, "Implementation of ransomware prediction system based on weighted-KNN and real-time isolation architecture on SDN Networks," *2019 IEEE Int. Conf. Consum. Electron. - Taiwan, ICCE-TW 2019*, pp. 2–3, 2019, doi: 10.1109/ICCE-TW46550.2019.8991771.

[14] A. Maheshwari, B. Mehraj, M. S. Khan, and M. S. Idrisi, "Microprocessors and Microsystems An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment," vol. 89, no. December 2021, 2022.

[15] R. Priyadarshini and R. K. Barik, “A deep learning based intelligent framework to mitigate DDoS attack in fog environment,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2019, doi: 10.1016/j.jksuci.2019.04.010.

[16] M. F. Fibrianda and A. Bhawiyuga, “Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 9, pp. 3112–3123, 2018.

[17] S. R. Afif, P. Sukarno, and M. A. Nugroho, “Analisis Perbandingan Algoritma Naive Bayes dan Decision Tree untuk Deteksi Serangan Denial of Service (DoS) pada Arsitektur Software Defined Network (SDN),” *e-Proceeding Eng.*, vol. 5, no. 3, pp. 7515–7521, 2018.

[18] M. M. Azis, Y. Azhar, and S. Syaifuddin, “Analisa Sistem Identifikasi DDoS Menggunakan KNN Pada Jaringan Software Defined Network(SDN),” *J. Repos.*, vol. 2, no. 7, p. 915, 2020, doi: 10.22219/repositor.v2i7.762.

[19] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, “DDoS attack detection and classification via Convolutional Neural Network (CNN),” *Proc. - 2019 IEEE 9th Int. Conf. Intell. Comput. Inf. Syst. ICICIS 2019*, pp. 233–238, 2019, doi: 10.1109/ICICIS46948.2019.9014826.

[20] P. Preamthaisong, A. Auyporntrakool, P. Aimtongkham, T. Sriwuttisap, and C. So-In, “Enhanced ddos detection using hybrid genetic algorithm and decision tree for SDN,” *JCSSE 2019 - 16th Int. Jt. Conf. Comput. Sci. Softw. Eng. Knowl. Evol. Towar. Singul. Man-Machine Intell.*, pp. 152–157, 2019, doi: 10.1109/JCSSE.2019.8864216.

[21] J. Cui, M. Wang, Y. Luo, and H. Zhong, “DDoS detection and defense mechanism based on cognitive-inspired computing in SDN,” *Futur. Gener. Comput. Syst.*, vol. 97, pp. 275–283, 2019, doi: 10.1016/j.future.2019.02.037.

[22] J. David and C. Thomas, “Detection of distributed denial of service attacks

based on information theoretic approach in time series models," *J. Inf. Secur. Appl.*, vol. 55, no. October, p. 102621, 2020, doi: 10.1016/j.jisa.2020.102621.

[23] S. Deng, X. Gao, Z. Lu, Z. Li, and X. Gao, "DoS vulnerabilities and mitigation strategies in software-defined networks," *J. Netw. Comput. Appl.*, vol. 125, no. June 2018, pp. 209–219, 2019, doi: 10.1016/j.jnca.2018.10.011.

[24] R. F. Fouladi, O. Ermiş, and E. Anarim, "A DDoS attack detection and defense scheme using time-series analysis for SDN," *J. Inf. Secur. Appl.*, vol. 54, no. August, p. 102587, 2020, doi: 10.1016/j.jisa.2020.102587.

[25] R. Swami, M. Dave, and V. Ranga, "Defending DDoS against Software Defined Networks using Entropy," *Proc. - 2019 4th Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2019*, pp. 1–5, 2019, doi: 10.1109/IoT-SIU.2019.8777688.

[26] T. Lotlikar and D. Shah, "A Defense Mechanism for DoS Attacks in SDN (Software Defined Network)," *2019 Int. Conf. Nascent Technol. Eng. ICNTE 2019 - Proc.*, no. Icnte, pp. 1–7, 2019, doi: 10.1109/ICNTE44896.2019.8945900.

[27] Y. Cui *et al.*, "Towards DDoS detection mechanisms in Software-Defined Networking," *J. Netw. Comput. Appl.*, vol. 190, no. June, p. 103156, 2021, doi: 10.1016/j.jnca.2021.103156.

[28] B. Bouyeddou, F. Harrou, Y. Sun, and B. Kadri, "Detection of smurf flooding attacks using Kullback-Leibler-based scheme," *2018 4th Int. Conf. Comput. Technol. Appl. ICCTA 2018*, pp. 11–15, 2018, doi: 10.1109/CATA.2018.8398647.

[29] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Comput. Sci. Rev.*, vol. 39, p. 100332, 2021, doi: 10.1016/j.cosrev.2020.100332.

[30] Y. Liu, Y. Mu, K. Chen, Y. Li, and J. Guo, “Daily Activity Feature Selection in Smart Homes Based on Pearson Correlation Coefficient,” *Neural Process. Lett.*, no. 0123456789, 2020, doi: 10.1007/s11063-019-10185-8.

[31] H. Zhou, Z. Deng, Y. Xia, and M. Fu, “Author ’ s Accepted Manuscript A new Sampling Method in Particle Filter Based on Pearson Correlation Coefficient,” *Neurocomputing*, 2016, doi: 10.1016/j.neucom.2016.07.036.

[32] H. Zhu, “Multiple Ant Colony Optimization Based on Pearson Correlation Coefficient,” vol. 7, 2019.

[33] Y. Chen, J. Pei, and D. Li, “DETPro: A High-Efficiency and Low-Latency System Against DDoS Attacks in SDN Based on Decision Tree,” *IEEE Int. Conf. Commun.*, vol. 2019-May, pp. 1–6, 2019, doi: 10.1109/ICC.2019.8761580.

[34] J. Hu, H. Peng, J. Wang, and W. Yu, “kNN-P: A kNN classifier optimized by P systems,” *Theor. Comput. Sci.*, vol. 817, pp. 55–65, 2020, doi: 10.1016/j.tcs.2020.01.001.

[35] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, “A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions,” *Electron.*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071177.