KLASIFIKASI SERANGAN SMURF DENIAL OF SERVICE DENGAN METODE ITERATIVE DICHOTOMISER 3 (ID3)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

M. KHOIR SEPTIAWAN

09011281722031

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

KLASIFIKASI SERANGAN SMURF DENIAL OF SERVICE DENGAN METODE ITERATIVE DICHOTOMISER 3 (ID3)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

M. KHOIR SEPTIAWAN

09011281722031

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

HALAMAN PENGESAHAN

KLASIFIKASI SERANGAN SMURF DENIAL OF SERVICE DENGAN METODE ITERATIVE DICHOTOMISER 3 (ID3)

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh :

M. KHOIR SEPTIAWAN

09011281722031

Indralaya, 27 Mei 2021

Mengetahui,

Pembimbing I	Pembimbing II
Deris Stiawan, M.T., Ph.D., IPU.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 19780617 200604 1 002	**NIP. 19870122 201504 1 002**

Ketua Jurusan Sistem Komputer 24/6/21

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

NIP. 19661203 200604 1 001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 27 Mei 2021

Tim Penguji :

1. **Ketua : Ahmad Zarkasi, S.T., M.T.**
2. **Sekretaris : Rendyansyah, S.Kom., M.T.**
3. **Penguji : Sarmayanta Sembiring, S.Si., M.T.**
4. **Pembimbing I : Deris Stiawan, M.T., Ph.D., IPU.**
5. **Pembimbing II : Ahmad Heryanto, S.Kom., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 19661203 200604 1 001

HALAMAN PERNYATAAN

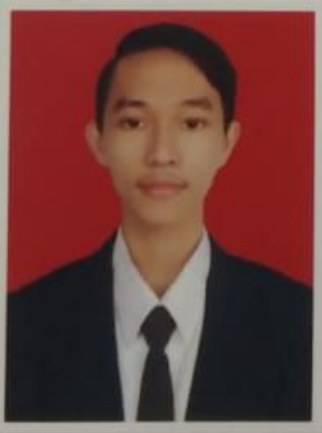
Yang bertanda tangan di bawah ini :

Nama	:	M. Khoir Septiawan
NIM	:	09011281722031
Program Studi	:	Sistem Komputer
Judul Penelitian	:	Klasifikasi Serangan Smurf Denial of Service Dengan Metode Iterative Dichotomiser 3 (ID3)

Hasil Pengecekan *Software iThenticate/Turnitin* : 4 %

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 tidak dipaksakan.



Indralaya, 27 Mei 2021

M. Khoir Septiawan

NIM. 09011281722031

HALAMAN PERSEMBAHAN

"Waktu bukan untuk bersantai, tapi santai juga memerlukan waktu. Waktu bukan untuk ditunggu, tapi waktu juga tak mau menunggu. Terima kasih waktu engkau selalu ada di setiap hariku."

"Waktu ibaratkan sebagai dua sisi mata pisau yang sama tajamnya. Di satu sisi dia bisa membuatmu berhasil dalam hidup, namun di sisi lain bisa saja membunuhmu secara perlahan."

"Terkadang waktu yang singkat memiliki kenangan yang hebat, dan terkadang kita di uji bukan untuk melihat kelemahan kita, tetapi untuk menentukan seberapa kuatnya kita."

"Jadilah seperti bunga teratai, sekalipun berada di lingkungan kotor, teratai tetap bersih dan menunjukkan keindahannya. Hal ini menggambarkan bahwa manusia sejatinya memang tetap membutuhkan satu sama lain, meski pada orang yang kurang baik sekalipun. Tapi, bukan berarti kamu harus mengikuti dan meniru kejelekan yang orang sekitarnya biasa lakukan."

"Jangan bandingkan prosesmu dengan proses orang lain, karena setiap bunga butuh waktu yang berbeda untuk mekar sempurna."

"Ada semangat yang harus tetap menyala, karena ada penyemangat yang harus dibuat bahagia yaitu kedua orangtua kita."

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis selalu panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat serta karunia-nya, sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul **"Klasifikasi Serangan Smurf Denial of Service Dengan Metode Iterative Dichotomiser 3 (ID3)"**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad Shallallahu 'Alaihi Wasallam beserta keluarga, sahabat dan para pengikutnya yang insha Allah istiqomah hingga akhir zaman.

Selesainya penyusunan laporan tugas akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusun laporan tugas akhir ini.
2. Orang Tua (Risultan, B.Sc. dan Asmawati, A.Ma., S.AP.) serta keluarga besar penulis yang tercinta yang selalu memberikan semangat serta do'a selama perkuliahan di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya sehingga dapat menyelesaikan laporan tugas akhir ini.
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 Universitas Sriwijaya.
5. Ibu Sri Desy Siswanti, S.T., M.T. selaku Pembimbing Akademik Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Deris Stiawan, M.T., Ph.D., IPU. selaku Pembimbing Tugas Akhir I Penulis Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing Tugas Akhir II Penulis Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

8. Mbak Nurul Afifa, M.Kom. yang telah membantu penulis dalam proses pengerjaan laporan Tugas Akhir ini.
9. Mbak Renny Virgasari, S.E. selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
10. Keluarga besar Lab Center of Excellent (CoE) dan teman-teman seperjuangan Konsentrasi Jaringan yang juga bimbingan dengan Bapak Deris Stiawan, M.T., Ph.D., IPU. dan Bapak Ahmad Heryanto, S.Kom., M.T.
11. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2017.
12. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
13. Almamater.

Penulis juga berterimakasih kepada semua pihak yang terlibat, baik secara langsung maupun tidak langsung dalam penyelesaian laporan tugas akhir ini.

Tentunya dalam pembuatan laporan tugas akhir ini, masih terdapat beberapa kekurangan dan kesalahan yang mungkin terjadi. Oleh karena itu sebagai bahan perbaikan kedepan penulis tentunya mengharapkan kritik, dan saran untuk perbaikan.

Akhir kata, semoga dengan pembuatan laporan tugas akhir ini, akan menjadi tambahan ilmu dan pengembangan wawasan kita terhadap sistem keamanan jaringan komputer. Semoga laporan tugas akhir ini dapat bermanfaat bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Indralaya, 27 Mei 2021
Penulis

M. Khoir Septiawan
NIM. 09011281722031

CLASSIFICATION SMURF ATTACKS DENIAL OF SERVICE USING ITERATIVE DICHOTOMISER 3 (ID3)

M. KHOIR SEPTIAWAN (09011281722031)

Computer Engineering Departement, Computer Science Faculty, Sriwijaya University

Email : khoir3000@gmail.com

ABSTRACT

Denial of Service (DoS) is an attack technique that is often carried out by attackers that aims to disable system capabilities. Denial of Service (DoS) attacks are a serious threat in today's networks, Smurf attack is an attack that can take advantage of the IP of the target host as a source of ICMP requests, as well as take advantage of the ICMP packet network protocol. In this case, the researcher uses the method of the supervised learning algorithm Iterative Dichotomiser 3 (ID3) which forms a tree model, this method will generate the entropy value as a sample of the test results on the node. In this study, there are 5 scenarios carried out on 2 different attack classes and 1 normal attack class with a total of 10 ID3 models and using 2 hyperparameter min sample leaf 100000 and hyperparameter max leaf nodes with a value of leaf 3 from pruning decision tree learning techniques. There are 10 ID3 models tested, the best model was obtained with 50% test data from max leaf nodes 3 and 80% test data from min sample leaf nodes 100000. The ID3 model has the highest evaluation in scenario 2 of the DoS attack class hyperparameter max leaf nodes 3 with sensitivity value 99.979%, precision 99.933%, specificity 99.989%, accuracy 99.982% and F1 99.956%.

Keywords : *Classification, Denial of Service (DoS), Smurf, Iterative Dichotomiser 3 (ID3).*

Acknowledged By,

Final Project Advisor I	***Final Project Advisor II***
Deris Stiawan, M.T., Ph.D., IPU.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 19780617 200604 1 002	**NIP. 19870122 201504 1 002**

The Head of Computer Systems Department

10/6/21

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

NIP. 19661203 200604 1 001

KLASIFIKASI SERANGAN SMURF DENIAL OF SERVICE DENGAN METODE ITERATIVE DICHOTOMISER 3 (ID3)

M. KHOIR SEPTIAWAN (09011281722031)

Jurusan sistem komputer, fakultas ilmu komputer, universitas sriwijaya

Email : khoir3000@gmail.com

ABSTRAK

Denial of Service (DoS) adalah teknik serangan yang sering dilakukan oleh *attacker* yang bertujuan untuk melumpuhkan kemampuan sistem. Serangan dari *Denial of Service* (DoS) merupakan ancaman yang serius dalam jaringan saat ini, Serangan *Smurf* merupakan serangan yang dapat memanfaatkan IP dari *Host* target sebagai sumber ICMP *Request*, serta mendapat keuntungan terhadap protokol jaringan paket ICMP. Pada kasus ini peneliti menggunakan metode dari *Supervised Learning* algoritma *Iterative Dichotomiser 3* (ID3) yang membentuk suatu model *Tree*, metode ini akan menghasilkan nilai *Entropy* sebagai sampel hasil pengujian pada *Node*. Pada penelitian ini ada 5 skenario yang dilakukan terhadap 2 kelas serangan yang berbeda dan 1 kelas serangan normal dengan jumlah 10 model ID3 dan menggunakan 2 *Hyperparameter Min Sample Leaf 100000* dan *Hyperparameter Max Leaf Nodes* dengan nilai *Leaf 3* dari teknik *Pruning Decision Tree Learning*. Dari 10 model ID3 yang diuji coba, model terbaik diperoleh dengan 50% data uji dari *Max Leaf Nodes 3* dan 80% data uji dari *Min Sample Leaf Nodes 100000*. Model ID3 memiliki evaluasi tertinggi pada skenario 2 kelas serangan DoS *Hyparameter Max Leaf Nodes 3* dengan nilai Sensitivitas 99,979%, Presisi 99,933%, Spesifisitas 99,989%, Akurasi 99,982% dan F1 99,956%.

Kata Kunci : Klasifikasi, Denial of Service (DoS), Smurf, Iterative Dichotomiser 3 (ID3).

Mengetahui,

Pembimbing I	**Pembimbing II**
Deris Stiawan, M.T., Ph.D., IPU.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 19780617 200604 1 002	**NIP. 19870122 201504 1 002**

Ketua Jurusan Sistem Komputer

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

NIP. 19661203 200604 1 001

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknik serangan yang sering dilakukan oleh *attacker* yang bertujuan untuk melumpuhkan kemampuan sistem dikenal sebagai serangan *Denial of Service* (DoS) [1]. Pengguna yang terkena serangan *Denial of Service* (DoS) akan mengalami akses layanan tidak normal [2], serta menyebabkan sumber daya pada jaringan, *processor* meningkat dalam jumlah yang sangat besar [3]. Serangan dari *Denial of Service* (DoS) merupakan ancaman yang serius dalam jaringan saat ini [4].

Serangan *Smurf* merupakan salah satu jenis serangan dari *Denial of Service* (DoS) yang dapat memanfaatkan IP dari *host* target sebagai sumber ICMP *request*, Serangan *Smurf* memanfaatkan keuntungan terhadap protokol jaringan paket ICMP [5]. Pada serangan *Denial of Service* (DoS) penyerang memanfaatkan lalu lintas jaringan yang berfokus pada target yang memiliki keamanan perangkat yang rendah [6].

Klasifikasi merupakan metode yang dimanfaatkan untuk menentukan kelas dari beberapa jenis kelas data, perolehan data tersebut akan menentukan data serangan [7], peneliti menggunakan teknik klasifikasi dari *machine learning* yang merupakan cara terbaik dalam menentukan fitur data menjadi kelas kelas yang sesuai [8].

Pada kasus ini peneliti menggunakan metode dari *supervised learning* yaitu *Iterative Dichotomiser 3* (ID3) yang membentuk suatu model *decision tree* [9], Bertujuan untuk membangun model yang akan memprediksikan suatu nilai dari variabel tujuan dan mempelajari *rules* sebuah keputusan sederhana dari *feature* [10]. Pada penelitian [11], berdasarkan hasil dari pengujian memanfaatkan algoritma dari *Iterative Dichotomiser 3* (ID3) memiliki hasil terbaik dalam tingkat akurasi yang didapatkan. Metode *Iterative Dichotomiser 3* (ID3) adalah algoritma dari *decision tree learning* yang digunakan untuk membentuk validasi model yang

paling dasar dan dikembangkan oleh *J. Ross Quinlan* [9], [10]. metode ini akan menghasilkan nilai *entropy* sebagai sampel hasil pengujian pada *node-node* [12].

Pada penelitian [5], membahas mengenai analisa terhadap serangan *smurf* dan POD memanfaatkan SVM sebagai metode analisa serangan. Pada penelitian tersebut peneliti masih manggunakan dataset dari KDD Cup DARPA 1999, menghasilkan prediksi kelas tingkat akurasi cukup besar. Disini peneliti akan mencoba menggunakan dataset dari CIC-IDS2018 dengan metode *Iterative Dichotomiser 3* (ID3). Pada penelitian [21], memanfaatkan metode K-NN sebagai klasifikasi jenis serangan *Denial of Service* (DoS) dan *Probing* pada *intrusi detection system* (IDS) menggunakan dataset KDD-Cup99 metode K-NN dari penelitian tersebut sangat bergantung pada nilai K untuk hasil klasifikasi.

Dari beberapa ulasan sumber penelitian tersebut peneliti tertarik menggambil judul pada penelitian [5], [21], [22], dan menggunakan dataset dari CSE-CIC-IDS2018 serta menggunakan *Iterative Dichotomiser 3* (ID3) sebagai metode penelitian. keunggulan menggunakan dataset CIC-IDS2018 tentunya menghasilkan serangan baru [23], [24] ,[25] dan *Iterative Dichotomiser 3* (ID3) merupakan algoritma pengambilan suatu keputusan secara menyeluruh dan menghitung berdasarkan kelas kelas tertentu [20].

1.2 Perumusan Masalah

Perumusan masalah berdasarkan hasil pada latar belakang yang telah dikemukakan, antara lain :

1. Bagaimana cara mengklasifikasikan serangan *Smurf Denial of Service* (DoS) ?
2. Bagaimana memilih *Hyperparameter Iterative Dichotomiser 3* (ID3) yang terbaik?
3. Bagaimana pengaruh *Iterative Dichotomiser 3* (ID3) terhadap akurasi, *recall*, spesifitas, presisi, *F1-Score*?

1.3 Batasan Masalah

Batasan masalah yang didapatkan pada penelitian tugas akhir ini, antara lain :

1. Penelitian ini hanya menggunakan data dari CSE-CIC-IDS2018.

2. Klasifikasi serangan *Smurf Denial of Service* (DoS) hanya dilakukan terhadap serangan Normal, *DoS-SlowHTTP* dan *DoS-Hulk*.
3. Penelitian ini hanya sebatas simulasi program dengan bahasa pemrograman *Python* untuk mengklasifikasikan serangan *Denial of Service* (DoS) dengan *Iterative Dichotomiser 3* (ID3) untuk validasi model.

1.4 Tujuan

Tujuan dari penelitian ini, antara lain :

1. Membangun model *Iterative Dichotomiser 3* (ID3) untuk melakukan klasifikasi pada serangan *Denial of Service* (DoS).
2. Menguji model *Iterative Dichotomiser 3* (ID3) dengan berbagai *Hyperparameter* untuk mendapatkan model *Iterative Dichotomiser 3* (ID3) terbaik.
3. Mendapatkan hasil terbaik dari performa akurasi, *recall*, spesifitas, presisi, *F1-Score*.

1.5 Manfaat

Manfaat dari penelitian ini, antara lain :

1. Dapat menggunakan algoritma *Iterative Dichotomiser 3* (ID3) sebagai klasifikasi serangan *Denial of Service* (DoS).
2. Dapat menggunakan *Hyperparameter* dari *Pruning Decision Tree Learning* untuk menghindari validasi model dan performa terbaik *(overfitting)* pada proses klasifikasi.
3. Dapat mengetahui seberapa baik validasi performa yang dihasilkan dari setiap *Hyperparameter Iterative Dichotomiser 3* (ID3).

1.6 Metodologi Penelitian

Metodologi penelitian yang peneliti gunakan pada tugas akhir ini antara lain:

1.6.1 Tahapan Pertama (Persiapan Data)

Pada tahapan ini peneliti menganalisa dan memahami bentuk data yang digunakan agar sesuai topik penelitian.

1.6.2 Tahapan Kedua (Pengolahan Data)

Pada tahapan ini peneliti melakukan pengolahan terhadap data yang akan diproses dengan model *machine learning*. Data diolah dengan cara mengekstraksi fitur serangan sebelum klasifikasi dengan metode *Iterative Dichotomiser 3* (ID3).

1.6.3 Tahapan Ketiga (Ekstraksi Fitur)

Pada tahapan ini menjelaskan proses dalam mengekstraksi fitur serangan *log* dan *pcap* menjadi format data *csv* menggunakan CICFlowMeter.

1.6.4 Tahapan Keempat (Klasifikasi)

Pada tahapan ini melakukan klasifikasi terhadap serangan *Denial of Service* (DoS) menggunakan beberapa *Hyperparameter* sebagai pengujian untuk validasi model *Iterative Dichotomiser 3* (ID3).

1.6.5 Tahapan Kelima (Analisa dan Kesimpulan)

Pada tahapan ini hasil evaluasi pada pengujian dengan *Hyperparameter* guna memvalidasikan model *Iterative Dichotomiser 3* (ID3). melakukan analisa dari hasil performa yang telah diperoleh dari setiap *Hyperparameter* selanjutnya menarik kesimpulan.

1.7 Sistematika Penelitian

Sistematika penelitian yang digunakan oleh peneliti pada tugas akhir ini, antara lain :

BAB I PENDAHULUAN

Pada bab bagian pertama berisikan paparan secara sistematis latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab tugas akhir bagian kedua berisikan penjelasan teori dasar yang menunjang penelitian ini. Dasar teori tersebut membahas literatur terhadap *Denial of Service* (DoS), serangan *Smurf, Decision Tree, Iterative Dichotomiser 3* (ID3).

BAB III METODOLOGI PENELITIAN

Pada bab penelitian bagian ketiga ini menjelaskan bagaimana proses saat menjalankan penelitian, dimulai dari tahap persiapan data, pengolahan data, ekstraksi fitur, klasifikasi model *Iterative Dichotomiser 3* (ID3), pembagian data latih dan uji dengan beberapa *Hyperparameter* dan validasi performa.

BAB IV HASIL DAN PEMBAHASAN

Pada bab bagian empat pada penelitian ini menjelaskan perolehan hasil dan analisa akhir dari penelitian yang telah dilakukan sebelumnya oleh peneliti.

BAB V KESIMPULAN

Pada bab yang kelima ini merupakan bagian kesimpulan berdasarkan perolehan dari hasil dan analisa pada evaluasi pengujian terhadap penelitian telah selesai dilakukan.

DAFTAR PUSTAKA

[1] G. B. Gunawan, P. Sukarno, and A. G. Putrada, "Pendeteksian Serangan *Denial of Service* (DoS) pada Perangkat Smartlock Berbasis Wifi Menggunakan SNORT IDS," *Issn*, vol. 5, no. 3, pp. 7875–7884, 2018.

[2] R. N. Wibowo, P. Sukarno, and E. M. Jadied, "Pendeteksian Serangan DoS Menggunakan Multiclassfier Pada NSL-KDD Dataset Pendahuluan Studi Terkait Penelitian tentang perbandingan waktu build model antara SVM dengan Naive Bayes," *e-Proceeding Eng.*, vol. 5, no. 3, pp. 7885–7893, 2018.

[3] P. Studi, S. Teknik, F. Informatika, and U. Telkom, "Deteksi Serangan *Denial of Service* (DoS) menggunakan Algoritma Probabilistic Neural Network (PNN)," vol. 6, no. 2, pp. 8808–8818, 2019.

[4] B. Jaya, Y. Yunus, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan *Denial of Service* (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, pp. 5–9, 2020, doi: 10.37034/jsisfotek.v2i4.81.

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

[6] K. Hayawi, Z. Trabelsi, S. Zeidan and M. M. Masud, "Thwarting ICMP Low-Rate Attacks Against Firewalls While Minimizing Legitimate Traffic Loss," in IEEE Access, vol. 8, pp. 78029-78043, 2020, doi: 10.1109/ACCESS.2020.2987479.

[7] W. Muslehatin, M. Ibnu, and Mustakim, "Penerapan Naïve Bayes Classification untuk Klasifikasi Tingkat Kemungkinan Obesitas Mahasiswa Sistem Informasi UIN Suska Riau," *Semin. Nas. Teknol. Informasi, Komun. dan Ind.*, p. 7, 2017.

[8] A. P. Wibawa, M. Guntur, A. Purnama, M. F. Akbar, and F. A. Dwiyanto, "Metode-metode Klasifikasi," *Pros. Semin. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 1, pp. 134–138, 2018.

[9] I. R. Munthe and V. Sihombing, "Klasifikasi Algoritma Iterative Dichotomizer (ID3) untuk Tingkat kepuasan pada Sarana Laboratorium Komputer," *J. Teknol. dan Ilmu Komput. Prima*, vol. 1, no. 2, pp. 27–34,

2018, doi: 10.34012/jutikomp.v1i2.237.

[10] M. Hutasuhut, D. Octavina, and J. Halim, “Penerapan Data Mining dalam Menganalisa Pola Kelayakan Siswa Pada Kelas Unggulan Menggunakan Algoritma Iterative Dichotomiser 3 (ID3) pada,” vol. 18, no. 2, pp. 154–160, 2019.

[11] H. Hikmatulloh, A. Rahmawati, D. Wintana, and D. A. Ambarsari, “Penerapan Algoritma Iterative Dichotomiser Three (Id3) Dalam Mendiagnosa Kesehatan Kehamilan,” *Klik - Kumpul. J. Ilmu Komput.*, vol. 6, no. 2, p. 116, 2019, doi: 10.20527/klik.v6i2.189.

[12] A. Surabaya, “Indonesian Journal of Science Learning,” vol. 1, no. 1, pp. 32–36, 2020.

[13] C. A. Winanto, “Deteksi serangan *Denial of Service* mengunakan Artificial Immune System,” *Comput. Eng.*, vol. 2, no. Faculty of Computer Science, Sriwijaya University, pp. 1–57, 2017.

[14] M. A. Fauzi, I. Ahmad, T. Hanuranto, and C. Setianingsih, “Sistem Deteksi Intrusi Menggunakan Algoritma Genetik Pada Intrusion Detection System Using Genetic Algorithm on DoS Attack in Tcp and Udp Protocol,” vol. 6, no. 2, pp. 4800–4807, 2019.

[15] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, “REATO: REActing TO *Denial of Service* attacks in the Internet of Things,” *Comput. Networks*, vol. 137, no. March, pp. 37–48, 2018, doi: 10.1016/j.comnet.2018.03.020.

[16] A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag, “A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid,” *IEEE Access*, vol. 8, pp. 177447–177470, 2020, doi: 10.1109/access.2020.3026923.

[17] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, “A survey of distributed denial-of-service attack, prevention, and mitigation techniques,” *Int. J. Distrib. Sens. Networks*, vol. 13, no. 12, 2017, doi: 10.1177/1550147717741463.

[18] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, “Survey on SDN based network intrusion detection system using machine learning approaches,” *Peer-to-Peer Netw. Appl.*, vol. 12, no. 2, pp. 493–501, 2019,

doi: 10.1007/s12083-017-0630-0.

[19] Primartha, R., Adhi Tama, B., Arliansyah, A., & Januar Miraswan, K. (2019). Decision Tree Combined with PSO-Based Feature Selection for Sentiment Analysis. Journal of Physics: Conference Series, https://doi.org/10.1088/1742-6596/1196/1/012018

[20] B. A. Putra, E. Sutinah, S. Hidayatulloh, and E. F. Imaduddin, "Keputusan Persetujuan Kredit Motor Menggunakan Algoritma Iterative Dichotomiser 3 (ID3)," *Inf. Syst. Educ. Prof.*, vol. 4, no. 1, pp. 13–24, 2019.

[21] 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.

[22] K. Kurniabudi, A. Harris, and A. Rahim, "Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest," *Techno.Com*, vol. 19, no. 1, pp. 56–66, 2020, doi: 10.33633/tc.v19i1.2860.

[23] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-January, no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[24] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *ICT Express*, vol. 5, no. 3, pp. 211–214, 2019, doi: 10.1016/j.icte.2019.03.003.

[25] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *ICT Express*, no. xxxx, 2020, doi: 10.1016/j.icte.2020.12.004.

[26] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," *ICISSP 2017 - Proc. 3rd Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2017-January, no. September, pp. 253–262, 2017, doi: 10.5220/0006105602530262.