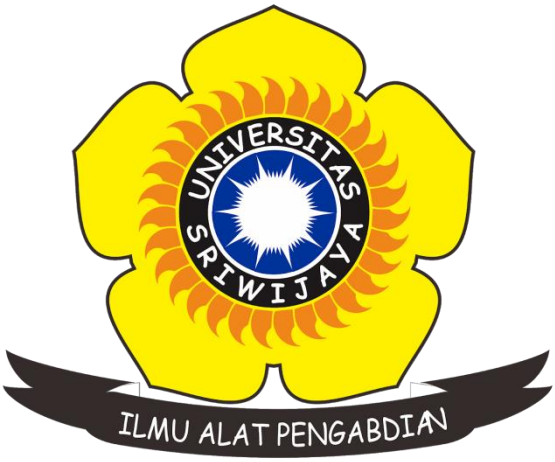
IMPLEMENTASI *MUTUAL INFORMATION CLASSIFIER* PADA SERANGAN *PORTSCAN* DENGAN METODE *SUPPORT VECTOR MACHINE* (SVM)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer



OLEH :

AHMAD RIFQI AKHDAN

09011381924098

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN

IMPLEMENTASI *MUTUAL INFORMATION CLASSIFIER* PADA SERANGAN *PORTSCAN* DENGAN METODE *SUPPORT VECTOR MACHINE* (SVM)

PROPOSAL TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh

AHMAD RIFQI AKHDAN

09011381924098

Palembang , 27 Juli 2023

Mengetahui,

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Jumat**

Tanggal : **7 Juli 2023**

Tim Penguji :

1. **Ketua** : **Huda Ubaya, M.T.**
2. **Sekretaris** : **Iman Saladin B Azhar, M.MSI**
3. **Penguji** : **Deris Setiawan, M.T., Ph.D.**
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 : Ahmad Rifqi Akhdan

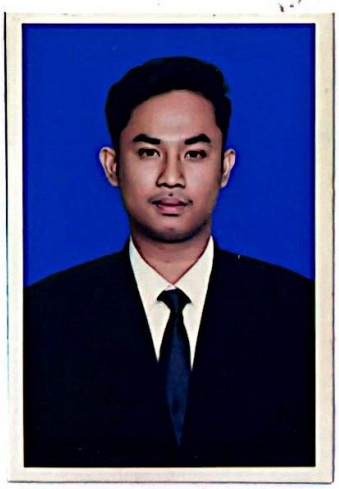
NIM : 09011381924098

Judul : Implementasi *Mutual Information Classifier* Pada Serangan *PortScan* Dengan Metode *Support Vector Machine* (SVM)

Hasil Pengecekan Plagiat/Turnitin : 19%

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, 7 Juli 2023

Ahmad Rifqi Akhdan

NIM. 09011381924098

HALAMAN PERSEMBAHAN

"**Jalanin apa yang kamu inginkan, jangan tergantung dari kata orang lain. Sehingga perjalananmu nanti akan memuahkan hasil dengan perih payahmu."**

Penulis:

"Ahmad Rifqi Akhdan"

Skripsi ini saya persembahkan untuk :

Kedua orang tua saya tercinta yang telah memberikan dukungan dan motivasi pada pembuatan skripsi ini maupun materil dan selalu memanjatkan doa yang luar biasa untuk anaknya ini. Saya sangat berterima kasih juga kepada teman-teman saya mau di BEM KM UNSRI Kabinet Akselerasi Juang, COMNETS, hingga teman perjuangan di kelas SK19 Bukit. Kalian semua yang telah mendorong saya dengan motivasi dan juga semangat yang diberikan hingga saya berada di titik ini.

"Motto Hidup"

"Awali harimu dengan senyuman"

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas kehadirat Tuhan Yang Maha Esa, yang atas segala berkat, kasih sayang, sertakarunia-Nya penulis dapat menyelesaikan penulisan proposal tugas akhir ini yang berjudul "**Implementasi *Mutual Information Classifier* Pada Serangan *PortScan* Dengan Metode *Support Vector Machine* (SVM)**".

Pada penyusunan laporan ini, penulis 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 kepada Tuhan Yang Maha Esa dan terimakasih kepada yang terhormat:

1. Kedua orang tua, saudara, dan Keluarga Besar yang selalu mendoakan dan memberikan motivasi dan *support.*
2. Bapak Alm. Dr. Jaidan Jauhari, S. pd. M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer.
4. Bapak Sarmayanta Sembiring, M.T. Selaku Dosen Pembimbing Akademik
5. Bapak Ahmad Heryanto, S. Kom, M.T. selaku Dosen Pembimbing Tugas Akhir.
6. Mba Sari selaku Administrasi Jurusan Sistem Komputer yang telah membantu melancarkan proses administrasi terkait Tugas Akhir
7. Teman Perjuangan BEM KM UNSRI Kabinet Akselerasi Juang
8. Seluruh teman yang ada di COMNETS
9. Seluruh staff dan pegawai jurusan sistem komputer beserta teman seperjuagan yang telah membersamai jalan juang.
10. Dan semua pihak yang telah membantu.

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis agar dapat segera diperbaiki sehingga laporan ini dapat dijadikan sebagai masukkan ide dan pemikiran yang bermanfaat bagi semua pihak dan menjadi tambahan bahan bacaan bagi yang tertarik dalam penelitian networking khususnya pada serangan *PortScan*.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, 7 Juli 2023

Penulis,

AHMAD RIFQI AKHDAN

NIM. 09011381924098

IMPLEMENTATION OF MUTUAL INFORMATION CLASSIFIER ON PORTSCAN ATTACKS WITH SUPPORT VECTOR MACHINE (SVM) METHOD

Ahmad Rifqi Akhdan (09011381924098)
Department of Computer Systems, Computer Science Faculty,
Sriwijaya University
Email : rifqiakhdan2@gmail.com

ABSTRACT

PortScan is an open port attack on machines connected to the network with an attack that can check for open ports. The dataset used in this research is the 2018 CIC-IDS from the Canadian Institute of Cybersecurity. This study discusses visualization of PortScan attacks on Mutual Information Classifier feature selection using the Support Vector Machine method. Then the researchers made a comparison between the Support Vector Machine and Kernel methods. From the results carried out by researchers, that the Kernel Radial Basis Function is very good with an average value of 99.53%.

Keywords : *PortScan, Mutual Information Classifier, Support Vector Machine, Kernel*

Palembang, 7 July 2023

Acknowledged,

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

IMPLEMENTASI *MUTUAL INFORMATION CLASSIFIER* PADA SERANGAN *PORTSCAN* DENGAN METODE *SUPPORT VECTOR MACHINE* (SVM)

Ahmad Rifqi Akhdan (09011381924098)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer. Universitas Sriwijaya
Email : rifqiakhdan2@gmail.com

ABSTRAK

PortScan merupakan serangan port yang terbuka pada mesin yang terhubung ke dalam jaringan dengan serangan yang dapat mengecek pada port terbuka. Dataset yang digunakan dalam penilitian ini adalah CIC-IDS 2018 yang berasal dari *Canadian Institute of Cybersecurity.* Penelitian ini membahas tentang visualisasi pada serangan *PortScan* pada seleksi fitur *Mutual Information Classifier* dengan metode *Support Vector Machine*. Kemudian peneliti melakukan perbandingan antara metode *Support Vector Machine* dan *Kernel*. Dari hasil yang dilakukan oleh peneliti, bahwa *Kernel Radial Basis Function* sangat baik dengan nilai rata-rata 99,53%.

Kata Kunci : *PortScan, Mutual Information Classifier, Support Vector Machine, Kernel*

Palembang, 7 Juli 2023

Mengetahui,

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, teknologi informasi telah mengalami kemajuan yang sangat pesat, terutama dengan adanya jaringan internet yang memudahkan dalam melakukan pekerjaan dan berkomunikasi dengan baik. Selain itu, akses terhadap informasi juga semakin mudah. Namun, keuntungan dari kemudahan tersebut tidak selalu positif, karena munculnya masalah seperti penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab demi keuntungan pribadi. Oleh karena itu, penting bagi pengguna untuk selalu berhati-hati dan memperhatikan keamanan informasi yang mereka akses dalam penggunaannya.

Data yang dimanfaatkan oleh pihak lain dapat mengakses informasi, sehingga orang tersebut dapat melakukan hal-hal yang diinginkan tanpa perizinan kita, maka data tersebut harus dijaga dengan baik, agar orang lain tersebut tidak bisa mengakses data-data yang kita miliki, seperti tidak menampilkan informasi data pribadi kita ke sosial media.

Penyalahgunaan data tersebut dapat dilakukan dengan tindakan kriminal seperti teknik serangan *Malware, Phising, Ransomware, Sql injection, Ddos,* dan *PortScan. PortScan* adalah port pada mesin yang terhubung ke dalam jaringan dengan analisa secara otomatis, yang terdapat memverifikasi pada port terbuka. Jenis-jenis teknik *PortScan* terdapat pada *stealth scan, SOCKS port probe, bounce scan, TCP scanning* dan *UDP scanning* [10].

Penjelasan diatas tersebut terdapat informasi tentang pelaksanaan terhadap serangan *PortScan* dengan metode *support vector machine,* yang dimana *support vector machine* merupakan salah satu metode dalam *machine learning* yang biasanya digunakan untuk klasifikasi dan regresi. Dalam pemodelan klasifikasi tersebut terdapat *support vector machine* memiliki konsep yang lebih matang dan jelas secara matematis dibandingkan dengan teknik-teknik klasifikasi lainnya. *support vector machine* adalah suatu sistem seperangkat pendekatan pembelajaran pada mesin yang akan digunakan untuk klasifikasi dan regresi. *Support vector machine* merupakan konsep bidang keputusan yang dapat mendefinisikan batas

keputusan. Bidang keputusan adalah salah satu yang memisahkan antara satu set objek yang memiliki keanggotaan kelas yang berbeda [8]. Manfaat pada *support vector machine* memiliki sebuah teknik untuk menemukan *hyperplane* pada memisahkan dua set data yang berbeda, dan keunggulannya untuk memastikan antara jarak dalam proses komputasi menjadi lebih cepat. *Mutual information classifier* merupakan sebuah teknik pada perhitungan dua variabel acak dari X dan Y, dengan variabel yang diperoleh dalam melakukan pengurangan acak-acak lainnya.

Penelitian tentang *PortScan* telah banyak dibahas sebelumnya, salah satunya pada jurnal yang berjudul "*Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms*". penelitian tersebut membahas perihal serangan *PortScan* dengan menggunakan metode *support vector machine* untuk mengatasi menghindari dari serangan *cyber*. Sehingga hasil pemindaian port tersebut dapat menunjukkan tingkat akurasi mencapai 97,80% serta 69,79%. Kelemahan pada jurnal tersebut, adanya dataset pada KDD99 yang sudah tua dan tidak bisa memberikan informasi jenis serangan baru. Sehingga penelitian mengganti dataset CIC-IDS2017 [1].

Dalam penelitian lain yang berjudul "*Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis*", disebutkan bahwa serangan seperti pemindaian port dan *Distributed Denial of Service* (DDoS) dapat mengakibatkan peretasan sistem dan pencurian informasi data. Penelitian tersebut juga menyimpulkan bahwa dengan menggunakan algoritma seperti *Support Vector Machine, K-Nearest Neighbors, Area Under Curve* (AUC), *Receiver Operating Characteristic* (ROC), dan *Principal Component Analysis* (PCA), pemindaian Port dan DDoS dapat diidentifikasi. Hasil dari analisis machine learning menunjukkan bahwa algoritma *Support Vector Machine* memiliki tingkat akurasi terbaik dengan hasil mencapai 90%. Namun, penelitian tersebut memiliki kelemahan yaitu validasi silang yang dilakukan hanya sebanyak 10 kali lipat, sehingga dapat membawa sedikit perubahan pada hasil akurasi rata-rata dari validasi silang. [5].

Penelitian lainnya yang berjudul "*Port Scan Identication Through Regression Applying Logistic Testing Methods to Balanced Data*". Penelitian

tersebut membahas mengidentifikasi serangan *PortScan* dengan metode *support vector machine* untuk melakukan beberapa tes dengan teknik penyeimbangan data untuk mencari hasil yang terbaik. Kelemahan pada peneliti tersebut bahwa nilai prediksi metode *NearMiss* lebih tinggi dibandingkan metode *SMOTE*, bahwa *SMOTE* lebih efisiensi dalam penerapan. Sehingga jurnal tersebut menggunakan dataset CIC-IDS2017 dengan hasil akurasi 97,80% dan 69,79% [7].

Penelitian lainnya juga yang berjudul "*Efficient Classification of Portscan Attacks using Support Vector Machine*". Penelitian tersebut membahas tentang serangan *PortScan* dengan dataset KDD'99, yang mana pada tahap pertama merupakan lalu lintas campuran secara keseluruhan yang diberikan sebagai input ke SVM, dan fase kedua merupakan algoritma pengurangan fitur yang diterapkan pada lalu lintas campuran dan diumpankan ke SVM. Kelemahannya terdapat data yang berlebihan, sehingga peneliti dapat melakukan validasi dua kali dengan waktu komputasi 7558,81. Hasil akurasi tesebut terdapat keseluruhan 99,7652% [8].

Adapun penelitian lainnya yang berjudul "*Detection of slow port scans in flow-based network traffic*". Penelitian tersebut membahas *PortScan* dengan dataset CIDDS-001 untuk pra-pemprosesan data pada aliran khusus untuk mendeteksi pemindaian port lambat, sehingga menghasilkan objek baru dengan berbasis aliran data untuk mempertimbangkan pengetahuan domain dan struktur jaringan. Peneliti mengatakan kelemahan tesebut adanya beberapa koleksi yang berisi aliran normal dan penyerang, sehingga peneliti menggunakan tambahan pelabelan koleksi campuran untuk ke penyerang kelas. Hasilnya menunjukkan adanya kedua pendekatan tersebut mampu mendeteksi pemindaian port yang lambat adanya alarm palsu yang amat rendah [11].

Berdasarkan latar belakang diatas, maka dapat dirumuskan masalah penelitian yang berjudul **"Implementasi *Mutual Information Classifier* Pada Serangan *PortScan* Dengan Metode *Support Vector Machine* (SVM)".**

1.2 Tujuan dan Manfaat

1.2.1 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu :

1. Menemukan poin tertinggi pada fitur seleksi *mutual information classifier* untuk pendeteksian serangan *PortScan* dengan dataset CIC-IDS2018.
2. Menganalisis keakuratan algoritma *support vector machine* terhadap serangan *PortScan* pada dataset CIC-IDS 2018.
3. Menerapkan Algoritma *support vector machine* dan *kernel* dengan pendeteksian serangan *PortScan* pada dataset CIC-IDS 2018.
4. Menampilkan akurasi dan mencari nilai terbaik dari metode *support vector machine* dan *kernel*.

1.2.2 Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu :

1 Dapat Mengetahui poin tertinggi pada fitur seleksi *mutual information classifier* pada sistem deteksi serangan *PortScan*.

2 Dapat mengimplementasikan dari algortima *support vector machine* pada pendeteksian serangan *PortScan* pada dataset CIC-IDS 2018.

3 Dapat memberikan informasi mengenai dataset *PortScan* yang digunakan dalam penelitian.

4 Dapat menampilkan akurasi dan mencari nilai terbaik dari metode *support vector machine* dan *kernel*.

1.3 Rumusan Masalah dan Batasan Masalah

1.3.1 Rumusan Masalah

Adapun rumusan masalah pada penelitian tersebut :

1. Bagaimana menemukan poin tertinggi pada fitur seleksi *mutual information classifier* dengan serangan *PortScan* pada dataset CIC-IDS 2018.

2. Bagaimana mengimplementasikan pada serangan *PortScan* dengan algoritma *support vector machine* pada dataset CIC-IDS 2018.

1.3.2 Batasan Masalah

Adapun batasan masalah pada penelitian tersebut :

1 Penelitian menggunakan dataset dari CIC-IDS 2018.
2 Algoritma yang digunakan dalam penelitian adalah algoritma *support vector machine.*

1.4 Sistematika Penulisan

Adapun dalam penyusunan penulisan tugas akhir ini yang disusun menjadi beberapa bab yang akan dijelaskan secara rinci dan mengenai apa yang dilakukan oleh penulis pada saat melakukan penelitian. Secara sistematis, tugas akhir ini disusun sebagai berikut:

BAB I PENDAHULUAN

Bagian BAB I berisi tentang sebuah latar belakang, tujuan dan manfaat, serta dalam perumusan masalah dan juga sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bagian BAB II berisikan tentang informasi seperti penelitian terdahulu yang telah dilakukan oleh peneliti sebelumnya, kajian literatur, serta juga terdapat landasan teori dari berbagai bahasan.

BAB III METODOLOGI PENELITIAN

Bagian BAB III berisikan tentang informasi pengumpulan data, spesifikasi *hardware* dan *software* yang digunakan, serta juga terdapat metode dan *flowchart* yang digunakan dalam penelitian.

BAB IV – PEMBAHASAN

Bagian BAB IV berisikan tentang pembahasan inti dari riset yang telah diselesaikan serta juga berisi mengenai analisis hasil dari riset tersebut.

BAB V – PENUTUP

Bagian BAB V yang merupakan bab akhir berisikan tentang seperti kesimpulan dan saran.

DAFTAR PUSTAKA

[1] D. Aksu and M. A. Aydin, “International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings,” *Int. Congr. Big Data, Deep Learn. Fight. Cyber Terror. IBIGDELFT 2018 - Proc.*, pp. 77–80, 2019.

[2] D. K. NURILAHI, R. MUNADI, S. SYAHRIAL, and A. BAHRI, “Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning,” *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 10, no. 2, p. 309, 2022, doi: 10.26760/elkomika.v10i2.309.

[3] R. Achmad, E. V. Manullang, and E. R. Sanmas, “Rancang Bangun Aplikasi Deteksi Dan Penanganan Serangan Ddos Dan Port Scanning Memanfaatkan Snort Pada Jaringan Komputer,” *J. Teknol. Inf.*, vol. 8, no. 1, pp. 2–11, 2020.

[4] M. Anif, S. Hws, and M. D. Huri, “Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang,” *J. TELE, Vol. 13 Nomor 1*, vol. 13, no. 1, pp. 25–30, 2015.

[5] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. A. . Usman, “Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis,” *Mehran Univ. Res. J. Eng. Technol.*, vol. 40, no. 1, pp. 215–229, 2021, doi: 10.22581/muet1982.2101.19.

[6] F. Saidi, Z. Trabelsi, and H. Ben Ghazela, “Fuzzy logic based intrusion detection system as a service for malicious port scanning traffic detection,” *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 2019-Novem, 2019, doi: 10.1109/AICCSA47632.2019.9035263.

[7] C. Alexandre, C. Tojeiro, C. D. J. Reis, K. Augusto, P. Da, and T. J. Lucas, “Port Scan Identi cation Through Regression Applying Logistic Testing Methods to Balanced Data Port Scan Identification Through Regression Applying Logistic Testing Methods to Balanced Data,” 2022.

[8] M. Vidhya, “Efficient classification of portscan attacks using Support Vector Machine,” *2013 Int. Conf. Green High Perform. Comput. ICGHPC 2013*, 2013, doi: 10.1109/ICGHPC.2013.6533915.

[9] M. S. Kumar, J. Ben-Othman, K. G. Srinivasagan, and G. U. Krishnan, “Artificial Intelligence Managed Network Defense System against Port Scanning Outbreaks,” *Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019*, pp. 1–5, 2019, doi: 10.1109/ViTECoN.2019.8899380.

[10] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Surveying port scans and their detection methodologies,” *Comput. J.*, vol. 54, no. 10, pp. 1565–1581, 2011, doi: 10.1093/comjnl/bxr035.

[11] M. Ring, D. Landes, and A. Hotho, “Detection of slow port scans in flow-based network traffic,” *PLoS One*, vol. 13, no. 9, pp. 1–18, 2018, doi: 10.1371/journal.pone.0204507.

[12] M. Almseidin, M. Al-Kasassbeh, and S. Kovacs, “Detecting Slow Port Scan Using Fuzzy Rule Interpolation,” *2019 2nd Int. Conf. New Trends Comput. Sci. ICTCS 2019 - Proc.*, 2019, doi: 10.1109/ICTCS.2019.8923028.

[13] S. K. Patel and A. Sonker, “Internet Protocol Identification Number Based Ideal Stealth Port Scan Detection Using Snort,” *Proc. - 2016 8th Int. Conf. Comput. Intell. Commun. Networks, CICN 2016*, pp. 422–427, 2017, doi: 10.1109/CICN.2016.89.

[14] D. Hardan Gutama, A. Kenya, A. Estetikha, R. A. Setiawan, and A. A. Yogyakarta, “Penanganan Serangan Brute Force dan Port Scanning Pada Router Mikrotik,” *J. Sist. Informasi, dan Teknol. Inf.*, vol. 1, pp. 1–13, 2022, [Online]. Available: https://journal-siti.org/index.php/siti/PublishedByHPTAI.

[15] R. R. Singh and D. Singh Tomar, “Network Forensics: Detection and Analysis of Stealth Port Scanning Attack,” *Int. J. Comput. Networks Commun. Secur.*, vol. 3, no. 2, pp. 33–42, 2015.

[16] C. V. Neu, C. G. Tatsch, R. C. Lunardi, R. A. Michelin, A. M. S. Orozco, and A. F. Zorzo, "Lightweight IPS for port scan in OpenFlow SDN networks," *IEEE/IFIP Netw. Oper. Manag. Symp. Cogn. Manag. a Cyber World, NOMS 2018*, pp. 1–6, 2018, doi: 10.1109/NOMS.2018.8406313.

[17] M. Dabbagh, A. J. Ghandour, K. Fawaz, W. El-Hajj, and H. Hajj, "Slow port scanning detection," *Proc. 2011 7th Int. Conf. Inf. Assur. Secur. IAS 2011*, pp. 228–233, 2011, doi: 10.1109/ISIAS.2011.6122824.

[18] W. El-Hajj, F. Aloul, Z. Trabelsi, and N. Zaki, "On detecting port scanning using fuzzy based intrusion detection system," *IWCMC 2008 - Int. Wirel. Commun. Mob. Comput. Conf.*, pp. 105–110, 2008, doi: 10.1109/IWCMC.2008.19.

[19] R. R. Singh and D. S. Tomar, "Storage efficient capturing of port scanning attack traffic," *Int. J. Appl. Eng. Res.*, vol. 12, no. 22, pp. 12652–12658, 2017.

[20] A. Gupta and L. Sen Sharma, "Mitigation of DoS and Port Scan Attacks Using Snort," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 4, pp. 248–258, 2019, doi: 10.26438/ijcse/v7i4.248258.

[21] 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.

[22] G. Cheng and X. Tong, "Fuzzy clustering multiple kernel support vector machine," *Int. Conf. Wavelet Anal. Pattern Recognit.*, vol. 2018-July, pp. 7–12, 2018, doi: 10.1109/ICWAPR.2018.8521307.

[23] D. Irawan, E. B. Perkasa, Y. Yurindra, D. Wahyuningsih, and E. Helmud, "Perbandingan Klassifikasi SMS Berbasis Support Vector Machine, Naive Bayes Classifier, Random Forest dan Bagging Classifier," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 10, no. 3, pp. 432–437, 2021, doi: 10.32736/sisfokom.v10i3.1302.

[24] E. Susilowati, M. K. Sabariah, and A. A. Gozali, “Implementasi Metode Support Vector Machine untuk Melakukan Klasifikasi Kemacetan Lalu Lintas Pada Twitter,” *E-Proceeding Eng.*, vol. 2, no. 1, pp. 1478–1484, 2015.

[25] N. A. Susanti and M. Walid, “Klasifikasi Data Tweet Ujaran Kebencian Di Media Sosial,” vol. 6, no. 2, pp. 538–543, 2022.

[26] A. Patle and D. S. Chouhan, “SVM kernel functions for classification,” *2013 Int. Conf. Adv. Technol. Eng. ICATE 2013*, 2013, doi: 10.1109/ICAdTE.2013.6524743.