

36/S/TEKKOM-KCBR/PK.03.08/16/AGUSTUS/2024

**PERANCANGAN MODEL DETEKSI DDOS MENGGUNAKAN
ALGORITMA RANDOM FOREST DENGAN PEMBERITAHUAN CEPAT
MELALUI TELEGRAM**

SKRIPSI

diajukan untuk memenuhi sebagian syarat
untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer



oleh
Ardi Rahman Sidiq
NIM 2009780

**PROGRAM STUDI TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2024**

HALAMAN HAK CIPTA

**PERANCANGAN MODEL DETEKSI DDOS MENGGUNAKAN
ALGORITMA RANDOM FOREST DENGAN PEMBERITAHUAN CEPAT
MELALUI TELEGRAM**

oleh

Ardi Rahman Sidiq

NIM 2009780

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Teknik pada Program Studi Teknik Komputer

© Ardi Rahman Sidiq

Universitas Pendidikan Indonesia

2024

Hak Cipta dilindungi oleh Undang-Undang.

Skripsi ini tidak diperbolehkan seluruhnya atau sebagian, dengan dicetak ulang,
difotokopi, atau cara lainnya tanpa izin dari Penulis

HALAMAN PENGESAHAN SKRIPSI

Ardi Rahman Sidiq

**PERANCANGAN MODEL DETEKSI DDOS MENGGUNAKAN
ALGORITMA RANDOM FOREST DENGAN PEMBERITAHUAN CEPAT
MELALUI TELEGRAM**

disetujui oleh dan disahkan oleh:

Pembimbing I



Muhammad Taufik Dwi Putra, S.Tr.Kom., M.T.I.

NIP. 920200819940117101

Pembimbing 2

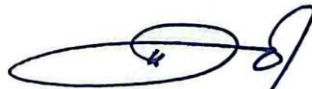


Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

Mengetahui,

Ketua Program Studi Teknik Komputer



Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

**HALAMAN PERNYATAAN
KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME**

Saya yang bertanda tangan dibawah ini:

Nama : Ardi Rahman Sidiq

NIM : 2009780

Program Studi : Teknik Komputer

Dengan ini saya menyatakan bahwa skripsi dengan judul "**PERANCANGAN MODEL DETEKSI DDOS MENGGUNAKAN ALGORITMA RANDOM FOREST DENGAN PEMBERITAHUAN CEPAT MELALUI TELEGRAM**" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Agustus 2024

Yang membuat pernyataan,



Ardi Rahman Sidiq

2009780

KATA PENGANTAR

Bismillahirrahmanirrahim

Segala puji dan syukur penulis panjatkan atas kehadiran Allah SWT, Tuhan Semesta Alam, yang selalu melimpahkan kasih sayang, rahmat, dan karunia-Nya kepada penulis. Tak lupa sholawat serta salam, semoga selalu tercurahkan kepada Baginda Nabi Muhammad SAW, beserta para keluarga, sahabat, dan para pengikutnya hingga akhir zaman. Alhamdulillahirabbil 'alamin atas segala berkah dan pertolongan-Nya, penulis mampu menyelesaikan skripsi ini yang berjudul **“PERANCANGAN MODEL DETEKSI DDOS MENGGUNAKAN ALGORITMA RANDOM FOREST DENGAN PEMBERITAHUAN CEPAT MELALUI TELEGRAM”** dengan baik dan tepat waktu.

Penulis menyadari bahwa skripsi ini sangat jauh dari kata sempurna, baik itu dari segi materi, susunan kalimat, ataupun dari tata bahasanya. Maka dari itu, dengan segala kerendahan hati, penulis mengharapkan kritik dan saran yang membangun, sehingga penulis dapat lebih baik lagi dalam penyusunan skripsi selanjutnya.

Demikian kata pengantar ini dibuat, semoga skripsi ini dapat memberikan manfaat bagi para pembaca dan semua pihak yang terlibat. Terima kasih.

Bandung, Agustus 2024

Penulis

HALAMAN UCAPAN TERIMA KASIH

Alhamdulillahirabbil 'alamin

Segala puji dan syukur penulis panjatkan atas kehadiran Allah Swt, Tuhan semesta alam, yang selalu melimpahkan kasih sayang, rahmat, dan karunia-Nya kepada penulis. Tak lupa selawat serta salam, semoga selalu tercurahkan kepada Baginda Nabi Muhammad saw, beserta para keluarga, sahabat, dan para pengikutnya hingga akhir zaman. Atas segala berkah dan pertolongan-Nya, penulis mampu menyelesaikan skripsi penelitian ini yang berjudul **“PERANCANGAN MODEL DETEKSI DDOS MENGGUNAKAN ALGORITMA RANDOM FOREST DENGAN PEMBERITAHUAN CEPAT MELALUI TELEGRAM”** dengan baik dan tepat waktu.

Dalam penyusunan skripsi ini, penulis banyak mendapat hambatan dan tantangan. Namun dengan dukungan dari berbagai pihak, penulis dapat menyelesaikan skripsi ini dengan baik. Untuk itu, penulis ingin sampaikan terima kasih kepada semua pihak yang telah memberikan bantuannya, terutama kepada yang terhormat:

1. Bapak Prof. Dr. Deni Darmawan, S.Pd., M.Si. M.Kom., MCE. selaku Direktur Universitas Pendidikan Indonesia di Cibiru
2. Ibu Dr. Yeni Yuniarti, M.Pd. Wakil Direktur Bidang Akademik dan Kemahasiswaan UPI Kampus Cibiru.
3. Bapak Dr. Jenuri, S.Ag, M.Pd. Wakil Direktur Bidang Sumber Daya dan Keuangan di UPI Kampus Cibiru
4. Bapak Annas Fachruddin Kasi Administrasi Umum dan Sumber Daya
5. Bapak Wirmanto Suteddy, S.T., M.T., selaku Dosen Wali yang telah dengan sabar dan ikhlas meluangkan waktunya untuk memberikan bimbingan, arahan, serta masukan yang membangun kepada penulis.
6. Bapak Muhammad Taufik Dwi Putra, S.Tr.Kom., M.T.I., selaku Dosen Pembimbing 1 yang telah dengan sabar dan ikhlas meluangkan waktunya untuk memberikan bimbingan, arahan, serta masukan yang membangun kepada penulis.

7. Bapak Dr. Eng. Munawir, S.Kom., M.T., selaku Dosen Pembimbing 2 yang telah dengan sabar dan ikhlas meluangkan waktunya untuk memberikan bimbingan, arahan, serta masukan yang membangun kepada penulis.
8. Bapak Deden Pradeka, S.T., M.Kom., selaku Ketua Program Studi Teknik Komputer yang telah dengan sabar dan ikhlas meluangkan waktunya untuk memberikan bimbingan, arahan, serta masukan yang membangun kepada penulis.
9. Bapak Anugrah Adiwilaga, S.ST., M.T., selaku Dosen Penguji 2 yang telah memberikan masukan dan arahan dalam menyempurnakan skripsi ini.
10. Seluruh Dosen dan Staff Akademik Universitas Pendidikan Indonesia Kampus Cibiru yang telah memberikan ilmu, bimbingan, serta bantuan selama penulis menjalankan studi.
11. Ibu Dedeh Juarliah, selaku Ibunda tercinta dari penulis yang tak pernah kenal lelah untuk selalu memberikan dukungan baik moril maupun materil kepada penulis, serta semangat dan doa yang selalu tercurah limpahkan untuk penulis.
12. Bapak Wawan Pahrul, selaku Ayahanda tercinta dari penulis yang tak pernah kenal lelah untuk selalu memberikan dukungan baik moril maupun materil kepada penulis, serta semangat dan doa yang selalu tercurah limpahkan untuk penulis.
13. Putri Nurul Hapsari, selaku Adik tercinta dan tersayang dari penulis yang menjadi motivasi dan alasan terbesar penulis agar dapat segera menyelesaikan studi.
14. Keluarga besar Bapak Dadang Ismail dan keluarga besar Bapak Epep Karyatun yang selalu memberikan dukungan, semangat, dan doa kepada penulis.
15. Syalwa Poetrie Chiekal Amalia, *special person, moodbooster*, kekasih hati, belahan jiwa, pujaan hati, sahabat, dan rumah untuk penulis yang selalu memberikan berbagai dukungan, semangat, bantuan, serta tak kenal lelah menemani penulis dalam menyusun rangkaian skripsi ini.
16. Fikri Rizalul Haq sebagai sahabat dan teman perkuliahan yang selalu hadir untuk memberikan semangat dan dorongan, serta menemani dalam setiap momen, baik suka maupun duka, sepanjang perjalanan kuliah ini.

17. Fanny Muhammad Fahmi Kamilah sebagai teman setia dalam menjalani perkuliahan, yang tak pernah berhenti memberikan dukungan dan motivasi, serta selalu ada di saat senang maupun susah selama masa kuliah ini.
18. Mohamad Rizal Hanafi sebagai rekan seperjuangan di bangku perkuliahan yang selalu siap memberikan dukungan moral dan motivasi, serta menemani dalam setiap langkah, baik di masa suka maupun duka sepanjang perkuliahan ini.
19. Teman-teman seperjuangan dan rekan-rekan perkuliahan yang selalu memberikan dukungan dan kebersamai baik saat suka maupun duka selama perkuliahan ini.
20. Pihak-pihak lainnya yang tidak dapat dituliskan satu per satu oleh penulis yang selama penyusunan skripsi ini telah banyak membantu penulis.

Penulis menyadari bahwa skripsi ini sangat jauh dari kata sempurna, baik itu dari segi materi, susunan kalimat, ataupun dari tata bahasanya. Maka dari itu, dengan segala kerendahan hati, penulis mengharapkan kritik dan saran yang membangun, sehingga penulis dapat lebih baik lagi dalam penyusunan karya tulis ilmiah selanjutnya. Akhir kata, terima kasih kepada seluruh pihak yang telah memberikan dukungan dan bantuan kepada penulis selama penyusunan skripsi ini. Semoga amal baik yang diberikan menjadi *washillah* penolong di dunia dan kelak di akhirat, *Aamiin ya Rabbal'aalamin*.

Bandung, Agustus 2024

Penulis

PERANCANGAN MODEL DETEKSI DDoS MENGGUNAKAN ALGORITMA RANDOM FOREST DENGAN PEMBERITAHUAN CEPAT MELALUI TELEGRAM

Ardi Rahman Sidiq

2009780

ABSTRAK

Melindungi sistem dari serangan *cyber* dan upaya tidak sah, termasuk penyusupan atau pemindaian, adalah fokus utama. Di Indonesia, hal ini diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Serangan DDoS adalah ancaman serius bagi keamanan jaringan, di mana penyerang mencoba menonaktifkan layanan dengan membanjiri target dengan lalu lintas besar. Penelitian ini bertujuan mengembangkan model deteksi DDoS menggunakan algoritma *Random Forest* dan dataset CICDDoS2019, mencakup 431.371 sampel, dengan 345.096 sampel (80%) untuk pelatihan dan 86.275 sampel (20%) untuk pengujian. *Random Forest* dibandingkan dengan SVM, KNN, dan LSTM untuk memastikan metode yang tepat. Berdasarkan pengukuran kinerja keempat metode tersebut, *Random Forest* dipilih karena akurasi 93%, meskipun sama tinggi dengan SVM, tetapi unggul dalam generalisasi dan mengurangi overfitting melalui banyak pohon keputusan, dibandingkan dengan KNN (92%) dan LSTM (82%). Proses penelitian meliputi pengumpulan data, pra-pemrosesan, dan ekstraksi fitur seperti volume lalu lintas (Gbps), jumlah paket per detik (pps), dan permintaan per detik (rps). *Generated* data juga digunakan, dengan variasi dalam 72 parameter serangan, termasuk *Protocol* (nilai 6 untuk TCP dan 17 untuk UDP), *Flow Duration* (2.000.000 hingga 5.000.000 mikrodetik), *Total Fwd Packets* (5.000 hingga 20.000 paket), dan *Flow Bytes/s* (8.000.000 hingga 20.000.000 *byte/s*) serta mengintegrasikan notifikasi cepat melalui *Telegram*. Evaluasi model menunjukkan akurasi, presisi, recall, dan f1 score sebesar 93% dalam mengklasifikasikan serangan DDoS dan rata-rata waktu pengiriman notifikasi 0,0174 detik. Penelitian ini berhasil merancang model *Random Forest* dan mampu mengidentifikasi serangan DDoS, serta dapat diintegrasikan dengan *Telegram* menggunakan bahasa pemrograman *Python* untuk notifikasi.

Kata Kunci: *Random Forest*, DDoS, deteksi serangan, *Telegram*, keamanan jaringan

DDOS DETECTION MODEL DESIGN USING RANDOM FOREST ALGORITHM WITH QUICK NOTIFICATION VIA TELEGRAM

Ardi Rahman Sidiq

2009780

ABSTRACT

Protecting systems from cyber attacks and unauthorized attempts, including intrusion or scanning, is a primary focus. In Indonesia, this is regulated by Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). DDoS attacks are a serious threat to network security, where attackers try to disable services by flooding targets with large traffic. This research aims to develop a DDoS detection model using the Random Forest algorithm and the CICDDoS2019 dataset, covering 431,371 samples, with 345,096 samples (80%) for training and 86,275 samples (20%) for testing. Random Forest is compared with SVM, KNN, and LSTM to ensure the appropriateness of the method. Based on performance measurements of the four methods, Random Forest was chosen because of its 93% accuracy, although it is the same as SVM, but is superior in generalization and reducing overfitting over many decision trees, compared to KNN (92%) and LSTM (82%). The research process includes data collection, pre-processing, and feature extraction such as traffic volume (Gbps), number of packets per second (pps), and requests per second (rps). Generated data is also used, with variations in 72 attack parameters, including Protocol (value 6 for TCP and 17 for UDP), Flow Duration (2,000,000 to 5,000,000 microseconds), Total Fwd Packets (5,000 to 20,000 packets), and Flow Bytes/s (8,000,000 to 20,000,000 bytes/s) as well as integrating fast notifications via Telegram. Model evaluation shows accuracy, precision, recall and f1 score of 93% in classifying DDoS attacks and an average notification sending time of 0.0174 seconds. This research succeeded in designing a Random Forest model and was able to identify DDoS attacks, and can be integrated with Telegram using the Python programming language for notifications.

Keywords: *Random Forest, DDoS, attack detection, Telegram, network security*

DAFTAR ISI

HALAMAN HAK CIPTA.....	i
HALAMAN PENGESAHAN SKRIPSI	ii
HALAMAN PERNYATAAN.....	iii
KATA PENGANTAR.....	iv
HALAMAN UCAPAN TERIMA KASIH.....	v
ABSTRAK.....	viii
ABSTRACT	ix
DAFTAR ISI	x
DAFTAR TABEL	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN	xiv
DAFTAR PERSAMAAN.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Penelitian.....	1
1.2 Rumusan Masalah Penelitian.....	3
1.3 Tujuan Penelitian	4
1.4 Batasan Penelitian.....	4
1.5 Manfaat Penelitian	5
1.5.1 Manfaat Teoritis	5
1.5.2 Manfaat Praktis.....	5
1.6 Struktur Organisasi Skripsi.....	6
BAB II KAJIAN PUSTAKA	7
2.1 Kajian Pustaka	7
2.1.1 Jaringan Komputer	7
2.1.2 <i>Server</i>	9
2.1.3 Keamanan Jaringan Komputer	12
2.1.4 Serangan <i>Distributed Denial of Service (DDoS)</i>	12
2.1.5 Jenis-Jenis Pendeteksian Serangan <i>Cyber</i>	14
2.1.6 <i>Machine Learning</i>	15
2.1.7 <i>Random Forest</i>	17

2.1.8	<i>Telegram</i>	19
2.2	Penelitian Terkait.....	19
BAB III METODE PENELITIAN.....		22
3.1	Metode Penelitian.....	22
3.1.1	Model Arsitektur Random Forest.....	30
3.1.2	<i>Flowchart</i> Perancangan Model.....	31
3.2	Model <i>Machine Learning</i>	32
3.3	Metode Evaluasi.....	33
BAB IV TEMUAN DAN PEMBAHASAN.....		36
4.1	Ekperimen dan Implementasi.....	36
4.1.1	Penentuan Algoritma dan Model.....	36
4.1.2	Proses Pelatihan dan Pengujian Model.....	38
4.2	Hasil Implementasi Algoritma <i>Random Forest</i>	39
4.2.1	Pelatihan dan Pengujian Model.....	39
4.2.2	Evaluasi Model.....	40
4.3	Implementasi Pemberitahuan Cepat Melalui <i>Telegram</i>	49
4.3.1	Proses Pengiriman Notifikasi Setelah Deteksi Serangan.....	49
4.3.2	Teknis Implementasi Integrasi dengan <i>Telegram</i>	49
4.3.3	Hasil Integrasi dengan <i>Telegram</i>	51
4.3.4	Hasil Pengujian Notifikasi.....	53
4.4	Pembahasan.....	55
4.4.1	Hasil Deteksi Serangan DDoS pada Skenario yang Disimulasikan.....	55
4.4.2	Analisis Performa Sistem pada Kondisi Nyata.....	55
4.4.3	Pemberitahuan Cepat Melalui <i>Telegram</i>	56
BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI.....		57
5.1	Simpulan.....	57
5.2	Implikasi.....	57
5.3	Rekomendasi.....	58
DAFTAR PUSTAKA.....		60
LAMPIRAN.....		64

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	19
Tabel 3.1 Deskripsi Arsitektur Random Forest.....	31
Tabel 4.1 Perbandingan Model SVM, KNN, Random Forest, dan LSTM	36

DAFTAR GAMBAR

Gambar 2.1 Serangan <i>Distributed Denial of Service</i> (DDoS) (Herza, 2020)	13
Gambar 2.2 <i>Machine Learning Types</i> (Bengkel TI, 2023)	17
Gambar 2.3 <i>Random Forest Arsitektur</i> (Medium, 2023)	18
Gambar 3.1 Alur Penelitian.....	22
Gambar 3.2 Dataset CICDDoS2019	24
Gambar 3.3 <i>Generated Data</i>	26
Gambar 3.4 Kode untuk mengirim notifikasi ke <i>Telegram</i>	28
Gambar 3.5 Arsitektur Model <i>Random Forest</i>	30
Gambar 3.6 <i>Flowchart</i> Perancangan Model	32
Gambar 4.1 Pelatihan dan Pengujian Model.....	40
Gambar 4.2 Hasil Evaluasi Model dengan Menggunakan Real Data	40
Gambar 4.3 Hasil Evaluasi Model dengan menggunakan Generated DDoS Data	42
Gambar 4.4 Model Performance Metrics	44
Gambar 4.5 Hasil Cross Validation Scores	46
Gambar 4.6 Confusion Matrix untuk Model Random Forest pada Data Uji	47
Gambar 4.7 Install Library Request	50
Gambar 4.8 Kode untuk Mengirim Notifikasi ke Telegram	50
Gambar 4.9 Tangkapan Layar Notifikasi Telegram.....	51
Gambar 4.10 Hasil Notifikasi Telegram 50 Percobaan dengan Jaringan Wifi	51
Gambar 4.11 Hasil Notifikasi Telegram 50 Percobaan dengan Jaringan 4G.....	52
Gambar 4.12 Hasil Notifikasi Telegram 50 Percobaan dengan Ethernet LAN	53
Gambar 4.13 Hasil Pengujian Notifikasi	54

DAFTAR LAMPIRAN

Lampiran 1. Jadwal Penelitian	64
Lampiran 2. Instrumen Penelitian	64
Lampiran 3. Dataset	65
Lampiran 4. Fitur yang Digunakan	65
Lampiran 5. Descriptive Statistics	67
Lampiran 6. Data Distribution	70
Lampiran 7. Histograms.....	71
Lampiran 8. Boxplots.....	71
Lampiran 9. Heatmap.....	72
Lampiran 10. Pre-Processing	72
Lampiran 11. Modelling.....	73
Lampiran 12. Simulasi Random DDoS Test Data	74
Lampiran 13. Hasil Evaluasi Model SVM, KNN dan LSTM.....	75
Lampiran 14. Hasil Pengujian Notifikasi <i>Telegram</i> dengan Jaringan <i>Wifi</i>	76
Lampiran 15. Hasil Pengujian Notifikasi <i>Telegram</i> dengan Jaringan 4G.....	76
Lampiran 16. Hasil Pengujian Notifikasi <i>Telegram</i> dengan <i>Ethernet LAN</i>	76

DAFTAR PERSAMAAN

<i>Akurasi</i> (1).....	34
<i>Presisi</i> (2)	34
<i>Recall</i> (3)	34
<i>F1 – Score</i> (4).....	34

DAFTAR PUSTAKA

- Aryanti, S., & Aspriyono, H. (2023). Pengembangan Sistem Keamanan Jaringan Wifi Berbasis Mikrotik Menggunakan Metode Network Development Life Cycle (NDLC). *Teknosia*, 17(2), 88-95. <https://ejournal.unib.ac.id/teknosia/article/view/31582>
- Astuti, I. K. (2020). Jaringan komputer.
- Avisyah, G. F., Putra, I. J., & Hidayat, S. S. (2023). Open Artificial Intelligence Analysis using ChatGPT Integrated with Telegram Bot. *Jurnal ELTIKOM*, 7(1), 60-66.
- Bengkel TI. (n.d.). Apa Itu Machine Learning? Jenis-jenis Machine Learning. Diakses pada 11 Juli 2024 dari <https://www.bengkelti.com/blog/apa-itu-machine-learning-jenis-jenis-machine-learning/>
- Fauzi, A., Utami, E., & Hartanto, A. D. (2023). DDoS Penerapan Random Forest dan Adaboost untuk Klasifikasi Serangan DDoS. *Journal on Education*, 5(3), 7925-7937.
- Fergina, A., Kom, M., Simatupang, D. S., ST, M., Dewi, D. D., Stat, M., & Mat, M. (2024). Buku Ajar Jaringan Komputer dan Keamanan. Kaizen Media Publishing. <https://journal.irpi.or.id/index.php/malcom/article/view/95>
- Harto, M. K., & Basuki, A. (2021). Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 5(4), 1329-1333.
- Hermawan, R. (2015). Analisis konsep dan cara kerja serangan komputer Distributed Denial of Service (DDoS). *Faktor Exacta*, 5(1), 1-14. https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/viewFile/186/177
- Heryana, N., Kom, M., Erkamim, M., Kom, S., Kom, M., Afif Zuhri Arfianto, S. T. M. T., ... & Irmawati, S. Pengenalan Dasar Jaringan Komputer. CV Rey Media Grafika.
- Herza. (n.d.). Apa Itu Serangan DDoS?. Diakses pada 10 Juli 2024 dari <https://herza.id/blog/apa-itu-serangan-ddos/>

- ITBOX. (n.d.). Topologi Bus. Diakses pada 10 Juli 2024 dari <https://itbox.id/blog/topologi-bus/>
- Juhana, D. A., Soecipto, S., & Amaliyah, A. (2021). Perancangan Sistem Keamanan Jaringan Menggunakan Mikrotik Router Pada Management Bandwidth Di Cv. Algi Pin Bandung. *Telematika*, 3(1), 29-44. <http://www.ojs.uninus.ac.id/index.php/Telematika/article/view/2119>
- Karim, A., Bangun, B., Purnama, I., Harahap, S. Z., Irmayani, D., Nasution, M., ... & Munthe, I. R. (2020). Pengantar teknologi informasi. Yayasan Labuhanbatu Berbagi Gemilang.
- Kurniabudi, K., Harris, A., & Rahim, A. (2020). Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest. *Techno. Com*, 19(1), 56-66.
- Lisanda, S., & Monang, S. (2023). Pemanfaatan Aplikasi Messaging Telegram@ Xkwavers Sebagai Media Komunikasi Fans K-Pop Dalam Meningkatkan Value Diri Dan Kesadaran Beragama (Studi Kasus Pada Anggota Gc Telegram@ Xkwavers). *Jurnal Indonesia: Manajemen Informasi dan Komunikasi*, 4(3), 1105-1112. <http://www.journal.amikindonesia.ac.id/index.php/jimik/article/view/339>
- Maulana, I., & Alamsyah, A. (2023). Optimalisasi Deteksi Serangan DDoS Menggunakan Algoritma Random Forest, SVM, KNN dan MLP pada Jaringan Komputer. *Indonesian Journal of Mathematics and Natural Sciences*, 46(2), 83-92.
- MrMaster907. (n.d.). Introduction: Random Forest Classification by Example. Medium. Diakses pada 12 Juli 2024 dari <https://medium.com/@mrmaster907/introduction-random-forest-classification-by-example-6983d95c7b91>
- Muni, A., Kom, S., & Kom, M. (2024). *Kriptografi Untuk Keamanan Sistem Informasi Copyright@ 2024 by Abdul Muni, S. Kom., M. Kom., dkk.* Penerbit Kbm Indonesia.
- Pai, V., & Adesh, N. D. (2021). Comparative analysis of machine learning algorithms for intrusion detection. In *IOP Conference Series: Materials Science*

- and Engineering* (Vol. 1013, No. 1, p. 012038). IOP Publishing.
<https://doi.org/10.1088/1757-899X/1013/1/012038>
- Pandu Pratama Putra, P., & Dafwen Toresa, D. (2021). Buku Ajar Keamanan Informasi Dan Jaringan Komputer.
- Prabowo, A., Piwari, B., Syahwali, A. J., & Sutabri, T. (2024). Analisis Penggunaan Smart Sistem WhatsApp Untuk Meningkatkan Efisiensi Kerja Profesional Muda. *IJM: Indonesian Journal of Multidisciplinary*, 2(1), 107-114.
<https://journal.csspublishing.com/index.php/ijm/article/view/577>
- Purnama, T. (2023). Implementasi Intrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi. *Jurnal Teknologi Informasi Dan Komunikasi*, 14(2), 358-369.
<https://ejurnal.provisi.ac.id/index.php/JTIKP/article/view/726>
- Putra, R. F., Mukhlis, I. R., Datya, A. I., Pipin, S. J., Reba, F., Al-Husaini, M., ... & Judijanto, L. (2024). *Algoritma Pembelajaran Mesin: Dasar, Teknik, dan Aplikasi*. PT. Sonpedia Publishing Indonesia.
- Rachmadi, T., & Kom, S. (2020). Mengenal apa itu internet of things (Vol. 1). Tiga Ebook.
- Raharja, A. R., ST, M., & Kom, M. (2024). *Keamanan Jaringan*. Penerbit Kbm Indonesia.
- Ramadhan, B., Firdaus, D., & Rafi, A. R. (2023). Teknik SMOTE Sebagai Solusi Imbalance Class dalam Model Deteksi Intrusi DDoS dengan Metode PCA-Random Forest. *MIND (Multimedia Artificial Intelligent Networking Database) Journal*, 8(1), 52-64.
- Ridho, F. (2017). Implementasi Log Dalam Forensik Router Terhadap Serangan Distributed Denial of Service (DDoS). *Jurnal TIMES*, 6(2), 15-21.
- Ryan, N. G. (2018). Basic computer networking (Vol. 3). XP Solution Surabaya.
- Santoso, J. D. (2019). Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *INFOS Journal-Information System Journal*, 1(3), 44-50. <https://ojs.amikom.ac.id/index.php/INFOSJournal/article/view/2350>
- Saputro, A. (2016). Implementasi Sistem Keamanan Jaringan Dengan Menggunakan Intrusion Detection Sistem (IDS) Studi Kasus: Universitas Satya Negara Indonesia (Doctoral dissertation, Universitas Satya Negara Indonesia).

- Saputra, A. M. A., Kharisma, L. P. I., Rizal, A. A., Burhan, M. I., & Purnawati, N. W. (2023). *Teknologi Informasi: Peranan TI dalam berbagai bidang*. PT. Sonpedia Publishing Indonesia.
- Satria, D. (2023). *Pengantar Teknik Komputer: Konsep dan Prinsip Dasar*. PT. Sonpedia Publishing Indonesia.
- Sepriano, S., & Sutanto, A. (2024). *Buku Ajar Pengenalan Jaringan Komputer*. PT. Green Pustaka Indonesia.
- Setiawan, A., Yanto, B., & Yasdomi, K. (2018). Logika Fuzzy Dengan MATLAB (Contoh Kasus Penelitian Penyakit Bayi dengan Fuzzy Tsukamoto). *Jayapangus Press Books*, i-217.
- Shahrul, A., & Wibawa, A. P. (2021). Choosing an Instant Messaging App: Security or Convenience? Comparison between Whatsapp and Telegram. *Buletin Ilmiah Sarjana Teknik Elektro*, 3(2), 115-121.
- Suwintana, I. K. (2013). Sistem Inferensi Fuzzy Mamdani Berbasis Web. *Jurnal Matrix*, 3(1).
- Syafrizal, M. (2020). *Pengantar jaringan komputer*. Penerbit Andi.
- Suryana, O. (2018). Server dan web server. no. August, 14-23.
- Vikram, A. (2020, June). Anomaly detection in network traffic using unsupervised machine learning approach. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)* (pp. 476-479). IEEE. <https://doi.org/10.1109/ICCES48766.2020.9137896>
- Zebua, R. S. Y., Khairunnisa, K., Hartatik, H., Pariyadi, P., Wahyuningtyas, D. P., Thantawi, A. M., ... & Kharisma, L. P. I. (2023). *Fenomena Artificial Intelligence (Ai)*. PT. Sonpedia Publishing Indonesia.
- Zen Munawar, S. T., Kom, S., Kom, M., Putri, N. I., Kharisma, I. L., Kom, M., ... & MM, M. (2023). *Keamanan Sistem Informasi: Prinsip Dasar, Teori, dan Rekayasa Penerapan Konsep*. Kaizen Media Publishing.
- Zees, M. E. M. (2023). *Implementasi Autogluon dalam Efisiensi Model Prediktif Machine Learning pada Dataset International Business Machines (IBM) Human Resource (HR) Analytics Employee Attrition* (Doctoral dissertation, Universitas Islam Indonesia).