OPTIMALISASI *MULTI-CLASSIFICATION* SERANGAN *CYBER* MENGGUNAKAN METODE K-NEAREST NEIGHBOR

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

ZULI YANTI

09011182025014

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

HALAMAN PENGESAHAN

OPTIMALISASI *MULTI-CLASSIFICATION* SERANGAN *CYBER* MENGGUNAKAN METODE K-NEAREST NEIGHBOR

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

ZULI YANTI

09011182025014

Indralaya, 4 April 2024

Mengetahui,

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

AUTHENTICATION PAGE

MULTI-CLASSIFICATION OPTIMIZATION CYBER ATTACKS USING METHODS K-NEAREST NEIGHBOR

SKRIPSI

Submitted To Complete One Of The Requirments For Obtaining A Bachelor's Degree In Computer Science

By :

ZULI YANTI

09011182025014

Indralaya, 9 April 2024

Acknowledge,

Head Of Computer System Department	Final Project Advisor
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 : 22 Maret 2024

Tim Penguji :

1. **Ketua : Dr. Firdaus, M.Kom**
2. **Sekretaris : Iman Saladin B. Azhar, M.MSI**
3. **Penguji : Huda Ubaya, M.T**
4. **Pembimbing : Ahmad Heryanto, S.Kom, M.T**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

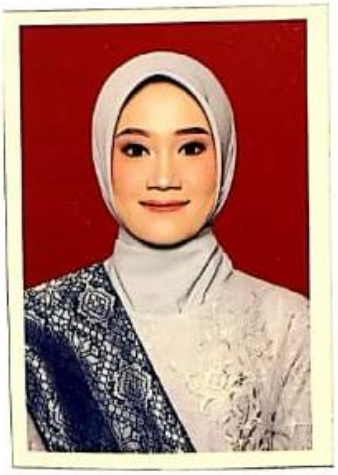
Yang Bertanda Tangan Di Bawah Ini :

Nama	:	Zuli Yanti
NIM	:	09011182025014
Judul	:	OPTIMALISASI *MULTI-CLASSIFICATION* SERANGAN *CYBER* MENGGUNAKAN METODE K-NEAREST NEIGHBOR

Hasil Pengecekkam Software iThenticate/Turnitin : 5%

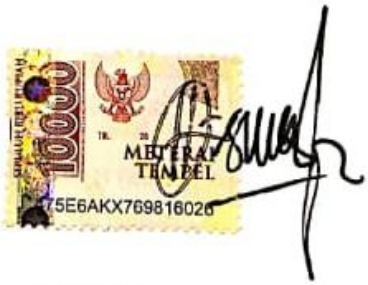
Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

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



Indralaya, 9 April 2024

Penulis,



Zuli Yanti

NIM.09011182025014

KATA PENGANTAR

Assalamualaikum Warahmatulahi Wabarakatuh

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT, karena berkat Rahmat dan Karunia-Nya lah sehingga penulis dapat menyelesaikan Laporan Tugas Akhir yang berjudul **"Optimalisasi Multi-Classification Serangan Cyber Menggunakan Metode K-Nearest Neighbor"**. Shalawat beriringkan salam senantiasa tercurahkan kepada Nabi Muhammad Shallallaahu 'Alaihi Wasallam yang telah membawa kedamaian dan rahmat untuk semesta alam serta menjadi suri tauladan bagi umatnya.

Pada kesempatan ini penulis menyampaikan banyak ucapan terimakasih kepada semua pihak yang telah membantu, memberikan motivasi, kemudahan, pengarahan, bimbingan, dorongan semangat, kritik dan saran selama proses penyusunan Tugas Akhir ini. Oleh karena itu, kesempatan ini penulis bersyukur dan mengucapkan banyak terima kasih kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat Kesehatan yang berlimpah.
2. Untuk diriku yang sudah berjuang dan melewati masalah – masalah yang sulit.
3. Kedua Orang Tua dan Keluarga yang selalu mendoakan serta memberikan motivasi dan semangat.
4. Bapak Prof. Dr. Erwin, S.Si., M.Si. Selaku Dekan Pengganti Antar Waktu Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Julian Supardi, S.Pd., M.T. selaku Wakil Dekan Bidang Akademik di Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Dr. Ir. H. Sukemi., M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Dr. Ahmad Zarkasi, M.T. selaku Dosen Pembimbing Akademik.

8. Bapak Ahmad Heryanto,S.Kom.,M.T. Selaku Dosen Pembimbing Tugas Akhir.
9. Bapak Yopi Syaputra selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
10. Para team MC yang selalu membantu dan menemani penulis dalam susah maupun senang selama penelitian ini.
11. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2020, yang sudah menjadi support system saya.
12. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta do'a.
13. Almamater.

Dalam penulisan Laporan Tugas Akhir ini penulis menyadari bahwa pada laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran dari semua pihak berkenan agar menjadi bahan evaluasi dan laporan ini menjadi lebih baik lagi dikemudian hari.

Akhir kata penulis ucapkan dan berharap semoga Laporan Tugas Akhir ini bermanfaat serta dapat memberikan pengetahuan dan wawasan bagi semua pihak yang membutuhkannya. Khususnya bagi mahasiswa/i Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Akhir kata saya ucapkan,

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Indralaya, 4 April 2024

Penulis,

Zuli Yanti

NIM. 09011182025014

OPTIMALISASI MULTI-CLASSIFICATION SERANGAN CYBER MENGGUNAKAN METODE K-NEAREST NEIGHBOR

ZULI YANTI

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : zuliyanti529@gmail.com

ABSTRAK

Serangan siber adalah bentuk ancaman yang bertujuan mencuri, merusak, atau mengubah data penting dalam sistem komputer atau jaringan. Jenis serangan ini meliputi peretasan, phising, dan malware. Mendeteksi serangan siber menjadi krusial untuk menjaga keamanan sistem informasi dari ancaman yang semakin meningkat. Salah satu alat yang digunakan untuk deteksi ancaman tersebut adalah Sistem Deteksi Intrusi (IDS), yang memantau peristiwa dalam sistem dan bertindak jika ada serangan atau perilaku mencurigakan. Dalam upaya meningkatkan kinerja IDS, penelitian telah mengeksplorasi penggunaan kecerdasan buatan (AI), terutama teknik Machine Learning (ML). Dalam penelitian ini, akan dibahas penerapan metode K-NN (K-Nearest Neighbors), suatu teknik nonparametrik untuk mengukur jarak antara data baru dengan data yang sudah diklasifikasikan sebelumnya menggunakan Euclidean distance. Untuk menguji keefektifan metode K-NN, berbagai dataset digunakan, termasuk UNSW-NB15, NSL-KDD, ISCX2012, dan CIC-IDS-2018. Hasil penelitian menunjukkan bahwa model berhasil mencapai tingkat akurasi yang tinggi pada masing-masing dataset selama proses pelatihan, yakni 88.00% pada dataset UNSW-NB15, 99.99% pada dataset NLS-KDD, 99.96% pada dataset ISCX2012, dan 92.00% pada dataset CIC-IDS-2018.

Kata Kunci : KNN, Serangan Siber, UNSW-NB15, NSL-KDD, ISCX2012, CIC-IDS-2018

Mengetahui,

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

MULTI-CLASSIFICATION OPTIMIZATION CYBER ATTACKS USING METHODS K-NEAREST NEIGHBOR

ZULI YANTI
Department of Computer Systems, Faculty of Computer Science, Sriwijaya University
Email : zuliyanti529@gmail.com

ABSTRACT

Cyber attacks are a form of threat aimed at stealing, damaging, or altering important data within computer systems or networks. These attacks include hacking, phishing, and malware. Detecting cyber attacks is crucial to maintaining the security of information systems from increasing threats. One tool used for threat detection is Intrusion Detection Systems (IDS), which monitor system events and take action if there are suspicious activities or attacks. In efforts to enhance IDS performance, research has explored the use of Artificial Intelligence (AI), particularly Machine Learning (ML) techniques. This study focuses on implementing the K-Nearest Neighbors (K-NN) method, a non-parametric technique for measuring the distance between new and previously classified data using Euclidean distance. To test the effectiveness of the K-NN method, various datasets are utilized, including UNSW-NB15, NSL-KDD, ISCX2012, and CIC-IDS-2018. The research findings indicate that the model achieves high accuracy rates on each dataset during the training process, namely 88.00% on the UNSW-NB15 dataset, 99.99% on the NSL-KDD dataset, 99.96% on the ISCX2012 dataset, and 92.00% on the CIC-IDS-2018 dataset.

Keywords: KNN, Cyber Attacks, UNSW-NB15, NSL-KDD, ISCX2012, CIC-IDS-2018.

Mengetahui,

Head Of Computer System Department	**Final Project Advisor**
Dr. Ir. Sukemi, M.T.	**Ahmad Heryanto, S.Kom, M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1. Latar Belakang

Ancaman serangan siber semakin serius bagi organisasi dan individu diseluruh dunia. Serangan siber merupakan jenis serangan yang ditujukan untuk merusak, mengubah, atau mencuri data penting pada komputer atau jaringan komputer. Serangan siber dapat berupa tindakan peretasan, phising, malware, dan berbagai jenis serangan lainnya [1]. Dampak dari serangan siber dapat menyebabkan kerugian finansial dan reputasi yang signifikan bagi individual atau organisasi yang menjadi korban. Oleh karena itu, penting bagi kita untuk mengembangkan sistem deteksi serangan siber yang efektif demi menjaga keamanan data dan sistem informasi.

Sistem deteksi serangan siber merupakan salah satu aspek penting dalam keamanan siber untuk melindungi sistem informasi dari ancaman serangan siber yang semakin meningkat [2]. Terkait laporan Badan Siber dan Sandi Negara (BSSN) mempublikasikan laporan tahunan berjudul "Monitoring Keamanan Siber" untuk tahun 2022. Laporan tersebut mengungkapkan bahwa terdapat lebih dari 900 juta atau tepatnya 973.952.290 anomali traffic atau serangan siber (*cyber attack*) yang terjadi diseluruh wilayah Indonesia sepanjang tahun 2022 [3]. Permintaan akan keamanan siber dan perlindungan terhadap anomali siber dan berbagai macam serangan, seperti akses tidak sah, Denial-Of-Service (DOS), phising, malware, botnet, spyware, worm dan sebagainya meningkat secara dramatis dalam beberapa hari terakhir [4]. Oleh karena itu dibutuhkan aplikasi yang mampu menganalisis data cerdas untuk memberikan pola perlindungan terhadap serangan dimasa depan.

Semakin meningkat serangan siber, membuat banyak para penelitian mencari cara bagaimana untuk mengatasi masalah serangan tersebut. Salah satunya adalah Intrusion Detection System (IDS). IDS merupakan suatu alat yang digunakan untu mendeteksi berbagai ancaman keamanan di komputer jaringan [5]. IDS akan memantau sebuah peristiwa yang aka terjadi didalam suatu sistem dan

mengambil tindakan pada peristiwa apakah disebut serangan atau tindakan yang sah dalam suatu sistem.

Untuk meningkatkan kinerja IDS, para peneliti telah mengeksplorasi penggunaan Artificial Intelligence (AI) dan lebih khusus lagi penerapan teknik berbasis Machine Learning (ML). ML merupakan cabang AI yang memberdayakan berbagai sistem kecerdasan yang dapat membuat komputer memiliki kemampuan dan kapasistas untuk memperbaiki proses pengambilan keputusan tanpa harus diprogram secara eksplisit [6]. Pada penelitian ini metode ML yang akan digunakan adalah ML berbasis Supervised Learning yakni K-Nearest Neighbor (KNN).

Metode K-NN merupakan metode klasisfikasi yang mengukur jarak antara data yang diberikan dan data yang telah diklasifikasikan sebelumnya. Algoritma K-NN merupakan teknik nonparametrik yang digunakan untuk melakukan klasifikasi dan regresi. Dalam regresi K-NN, algoritma KNN digunakan untuk memperkirakan variabel label kontinu [7]. Algoritma KNN merupakan suatu algoritma yang sering digunakan dalam klasifikasi, tujuan dari algoritma ini yaitu untuk mengklasifikasi suatu objek baru. Objek baru akan diklasifikasikan dengan cara mencari jarak terdekat ke objek pelatihan yang sudah ada berdasarkan pada rumus Euclidean distance. Setelah itu, objek baru akan diklasifikasikan kekelas yang paling banyak ditemukan diantara k tetangga terdekatnya [8] .

Serangan siber dapat dibagi menjadi berbagai kategori, dan untuk setiap kategori serangan, perlu digunakan teknik khusus untuk mendeteksinya. Oleh karena itu, didalam penelitian ini akan dikembangkan sistem deteksi *multi-classification* serangan siber dengan menggunakan metode K-NN. sistem deteksi ini akan mampu mendeteksi berbagai jenis serangan siber dengan menggunakan teknik yang berbeda untuk setiap jenis serangan [9]. Penelitian ini bertujuan untuk mengembangkan sistem deteksi serangan siber yang efektif dan dapat diandalkan. Diharapkan hasil penelitian ini dapat membantu organisasi dan individu dalam melindungi sistem informasi mereka dari ancaman serangan siber yang semakin meningkat.

Pada Penelitian [10] berdasarkan hasil yang didapatkan dari pemilihan fitur menggunakan algoritma genetika memiliki nilai fitnes sebesar 84,171% , dan fitur yang terpilih adalah 18 dari 41 fitur yang ada. Hasil evaluasi pengujian dengan

menggunakan dataset KDD-CUP 99 dengan metode K-NN, diperoleh akurasi data training 99,89% dan data testing sebesar 97,54%. Akurasi tersebut didapat pada paramater k = 5 sedangkan k = 7 rata-rata akurasi yang diperoleh adalah sebesar 97,52%. Akurasi hasil pengujian mmanual pada evaluasi k = 1,3,5,7, dan 9 dari 1000, 5000, 10000, 15000, dan 30000 didapat akurasi rata - rata 78,57%, 76,40%, 76,86%, 76,71%, dan 77,57%. Paramater tersebut memiliki tingkat akurasi tertinggi sebesar 78,57% pada parameter k = 1 dan tingkat akurasi terendah dengan akurasi sebesar 76,40% pada paramater k = 3.

Menurut penelitian [11] disebutkan bahwa beberapa algoritma seperti K-NN, Decision Tree, Logistic Regression, dan Random Forest telah. Hasil evaluasi menunjukkan bahwa algoritma K-NN memiliki performa terbaik dibandingkan dengan algoritma lainnya, dengan tingkat akurasi 95,51%, recall 89,42%, precision 89,42%. Sementara untuk hasil 10-fold cross validation, algoritma K-NN memiliki tingkat akurasi sebesar 93,61%, recall 85,05%, predicsion 85,25 dalam mendeteksi website malicious dan benign.

Berdasarkan pada uraian-uraian tersebut, penulis melakukan penelitian sistem deteksi serangan siber dengan menggunakan metode K-Nearest Neighbor pada dataset UNSW-NB15, NSL-KDD, ISCX-2012 dan CIC-IDS-2018 dan teknik multi-classification diharapkan mampu meningkatkan akurasi dan efektivitas deteksi serangan siber, serta dapat membantu melindungi sistem informasi dari ancaman serangan siber yang semakin meningkat. Itulah yang melatar belakangi penulis mengambil judul "**Optimalisasi *Multi-Classification* Serangan *Cyber* Menggunakan Metode K-Nearest Neighbor"**. Dikarenakan metode K-NN dianggap memperoleh tingkat akurasi yang baik dalam mengklasifikasikan sebuah data.

1.2. Tujuan

Tujuan dari penulisan Tugas Akhir ini adalah sebagai berikut :

1. Melakukan penerapan metode K-Nearest Neighbor dalam mendeteksi multi-classification serangan siber

2. Mencari tingkat akurasi terbaik, percision, recall dan F1- score dalam mendeteksi serangan siber dengan menggunakan metode K-NN pada sistem *deteksi multi-classification* serangan siber.

1.3. Manfaat

Adapun manfaat dari peulisan Tugas Akhir ini adalah sebagai berikut:

1. Dapat menerapkan metode K-Nearest Neighbor dalam mendeteksi multi-classification serangan siber.
2. Dapat memberikan informasi mengenai akurasi,precision, recall, dan F1-score menggunakan metode K-Nearest Neighbor dalam melakukan deteksi *multi-classification* serangan siber.

1.4. Perumusan Masalah

Adapun beberapa point rumusan masalah yang didapatkan dalam penulisan Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana cara melakukan deteksi multi-classification serangan siber dengan menggunakan metode K-Nearest Neighbor?
2. Bagaimana cara mencari tingkat akurasi terbaik, precision, recall dan F1-score dalam mendeteksi *multi-classification* serangan siber dengan menggunakan metode K-Nearest Neighbor?

1.5. Batasan Masalah

Batasan masalah merupakan batasan yang digunakan dalam penelitian agar penelitian tidak melenceng terlalu jauh. Dengan demikian batasan masalah dalam penyusunan Tugas Akhir ini sebagai berikut :

1. Penelitian ini hanya menggunakan dataset UNSW NB-15, NSL-KDD, ISCX-2012 dan CIC.IDS.2018.
2. Penelitian ini menggunakan program bahasa Python.
3. Algoritma klasifikasi yang digunakan dalam penelitian ini adalah Algoritma K-Nearest Neighbor.

4. Penelitian ini hanya menghasilkan output berupa akurasi terbaik, precision, recall, dan F1-score dalam mendeteksi *multi-classification* serangan siber dengan melihat kecocokan author dan tabel.

1.6. Metodologi Penelitian

Metodologi yang diterapkan dalam penyusunan Tugas Akhir ini melalui beberapa tahapan sebagai berikut :

1. Tahap pertama (Studi Pustaka)

   Tahap pertama yang akan dilakukan dalam penelitian ini adalah mencari sumber informasi, memahami, serta mempelajari kajian literatur dan referensi seperti buku, artikel yang terkait, maupun jurnal ilmiah yang berkaitan dengan serangan siber dan konsep dari metode K-Nearest Neighbor. Sehingga dapat memberikan penunjang pada metodologi yang akan diterapkan dalam penelitian ini.

2. Tahap Kedua (Perancangan Sistem)

   Pada tahap kedua membahas tentang perancangan sistem yang akan dilakukan dalam penelitian ini. Dimana, tahap ini akan membuat suatu perancangan menggunakan pemodelan simulasi dengan program bahasa Python.

3. Tahap Ketiga (Pengujian)

   Pada tahap ketiga ini adalah melakukan pengujian data. Tahap ini dilakukan jika semua sistem telah dibuat dan dikonfigurasi, maka akan dilakukan pengujian sesuai batasan masalah pada penelitian agar mendapatkan hasil yang optimal.

4. Tahap Keempat (Analisa)

   Selanjutnya pada tahap ini akan dilakukan analisa dari hasil tahap pengujian. Dimana pada tahap ini akan dilakukan analisa dari proses penelitian yang tujuannya untuk mengetahui kekurangan pada hasil perancangan dan faktor apa yang menjadi penyebabnya. Sehingga, bisa dilakukan pengembangan lagi untuk peneliti selanjutnya.

5. Tahap Kelima (Kesimpulan dan Saran)

   Tahap ini merupakan tahapan terakhir, dimana penulis melakukan penarikan kesimpulan yang berdasarkan studi pustaka, hasil perancangan sistem, serta hasil analisa penelitian. Dan memberikan saran untuk peneliti selanjutnya sebagai bahan referensi.

1.7. Sistematika Penulisan

Adapun penyusunan penulisan Tugas Akhir ini disusun menjadi beberapa sub bab yang akan dijelaskan secara rinci mengenai apa saja yang diakukan oleh penulis pada saat melakukan penelitian. Sistematika penulisan untuk Tugas Akhir ini disusun sebagai berikut:

BAB I PENDAHULUAN

Bab pertama berisi mengenai penjelasan secara sistematis berupa topik penelitian yang meliputi latar belakang, tujuan, manfaat, perumusan masalah, batasan masalah,metodologi yang digunakan dan terakhir mengenai sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab kedua akan menjelaskan dasar teori penelitian mengenai serangan siber, sistem deteksi multi-classification dan metode dari Algoritma K-Nearest Neighbor yang berkaitan langsung dengan penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ketiga berisi uraian secara sistematis bagaimana proses yang dilakukan dalam penelitian ini. Pada bab ini akan dilakukan pengkajian tahapan perancangan sistem dan bagaimana penerapan dari metode penelitian ini.

BAB IV PENGUJIAN DAN ANALISIS

Bab keempat akan menjelaskan hasil dari proses pengujian yang telah dilakukan, serta akan dilakukan analisis dari data yang didapat dari hasil pengujian.

BAB V KESIMPULAN DAN SARAN

Bab terakhir berisi mengenai kesimpulan dan saran dari hasil analisa yang diperoleh berdasarkan penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] M. A. Hasnat and M. Rahnamay-Naeini, “Detecting and locating cyber and physical stresses in smart grids using the k-nearest neighbour analysis of instantaneous correlation of states,” *IET Smart Grid*, vol. 4, no. 3, pp. 307–320, 2021, doi: 10.1049/stg2.12030.

[2] F. Zhao and Q. Tang, “A KNN learning algorithm for collusion-resistant spectrum auction in small cell networks,” *IEEE Access*, vol. 6, pp. 45796–45803, 2018, doi: 10.1109/ACCESS.2018.2861840.

[3] B. Publik, “D E S E M B E R 2 0 2 2 L a P O R a N,” no. 70, 2022, [Online]. Available: www.idsirtii.or.id

[4] I. H. Sarker, “Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects,” *Ann. Data Sci.*, 2022, doi: 10.1007/s40745-022-00444-2.

[5] H. M. Anwer, M. Farouk, and A. Abdel-Hamid, “A framework for efficient network anomaly intrusion detection with features selection,” *2018 9th Int. Conf. Inf. Commun. Syst. ICICS 2018*, vol. 2018-Janua, pp. 157–162, 2018, doi: 10.1109/IACS.2018.8355459.

[6] S. M. Kasongo, “An advanced intrusion detection system for IIoT Based on GA and tree based algorithms,” *IEEE Access*, vol. 9, pp. 113199–113212, 2021, doi: 10.1109/ACCESS.2021.3104113.

[7] K. Veena, K. Meena, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, “C SVM Classification and KNN Techniques for Cyber Crime Detection,” *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/3640017.

[8] Okfalisa, I. Gazalba, Mustakim, and N. G. I. Reza, “Comparative analysis of k-nearest neighbor and modified k-nearest neighbor algorithm for data classification,” *Proc. - 2017 2nd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2017*, vol. 2018-Janua, pp. 294–298, 2018, doi: 10.1109/ICITISEE.2017.8285514.

[9] B. B. Rao and K. Swathi, “Fast kNN Classifiers for Network Intrusion

Detection System," *Indian J. Sci. Technol.*, vol. 10, no. 14, pp. 1–10, 2017, doi: 10.17485/ijst/2017/v10i14/93690.

[10] M. A. Fauzi, A. T. Hanuranto, and C. Setianingsih, "Intrusion Detection System using Genetic Algorithm and K-NN Algorithm on Dos Attack," *2020 2nd Int. Conf. Cybern. Intell. Syst. ICORIS 2020*, pp. 3–8, 2020, doi: 10.1109/ICORIS50180.2020.9320822.

[11] G. A. Sandag, J. Leopold, and V. F. Ong, "Klasifikasi Malicious Websites Menggunakan Algoritma K-NN Berdasarkan Application Layers dan Network Characteristics," *CogITo Smart J.*, vol. 4, no. 1, pp. 37–45, 2018, doi: 10.31154/cogito.v4i1.100.37-45.

[12] K. Atefi, H. Hashim, and M. Kassim, "Anomaly analysis for the classification purpose of intrusion detection system with K-nearest neighbors and deep neural network," *Proceeding - 2019 IEEE 7th Conf. Syst. Process Control. ICSPC 2019*, no. December, pp. 269–274, 2019, doi: 10.1109/ICSPC47137.2019.9068081.

[13] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, no. August, pp. 99837–99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[14] M. Shorfuzzaman, "Detection of cyber attacks in IoT using tree-based ensemble and feedforward neural network," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, vol. 2020-Octob, pp. 2601–2606, 2020, doi: 10.1109/SMC42975.2020.9283443.

[15] L. Zhiqiang, G. Mohi-Ud-Din, L. Bing, L. Jianchao, Z. Ye, and L. Zhijun, "Modeling Network Intrusion Detection System Using Feed-Forward Neural Network Using UNSW-NB15 Dataset," *Proc. 2019 7th Int. Conf. Smart Energy Grid Eng. SEGE 2019*, pp. 299–303, 2019, doi: 10.1109/SEGE.2019.8859773.

[16] M. Zeeshan *et al.*, "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," *IEEE Access*, vol. 10, pp. 2269–2283, 2022, doi: 10.1109/ACCESS.2021.3137201.

[17] D. Jing and H. B. Chen, "SVM based network intrusion detection for the

UNSW-NB15 dataset," *Proc. Int. Conf. ASIC*, pp. 1–4, 2019, doi: 10.1109/ASICON47005.2019.8983598.

[18] Z. R. Tembusai, H. Mawengkang, and M. Zarlis, "K-Nearest Neighbor with K-Fold Cross Validation and Analytic Hierarchy Process on Data Classification," *Int. J. Adv. Data Inf. Syst.*, vol. 2, no. 1, pp. 1–8, 2021, doi: 10.25008/ijadis.v2i1.1204.

[19] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[20] S. N. Nguyen, V. Q. Nguyen, J. Choi, and K. Kim, "Design and implementation of intrusion detection system using convolutional neural network for DoS detection," *ACM Int. Conf. Proceeding Ser.*, pp. 34–38, 2018, doi: 10.1145/3184066.3184089.

[21] H. Liu, B. Lang, M. Liu, and H. Yan, "CNN and RNN based payload classification methods for attack detection," *Knowledge-Based Syst.*, vol. 163, pp. 332–341, 2019, doi: 10.1016/j.knosys.2018.08.036.

[22] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, "SSH and FTP brute-force attacks detection in computer networks: Lstm and machine learning approaches," *2020 5th Int. Conf. Comput. Commun. Syst. ICCCS 2020*, pp. 491–497, 2020, doi: 10.1109/ICCCS49078.2020.9118459.

[23] A. A. E. B. Donkol, A. G. Hafez, A. I. Hussein, and M. M. Mabrook, "Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks," *IEEE Access*, vol. 11, no. February, pp. 9469–9482, 2023, doi: 10.1109/ACCESS.2023.3240109.

[24] N. Gandhi, J. Patel, R. Sisodiya, N. Doshi, and S. Mishra, "A CNN-BiLSTM based Approach for Detection of SQL Injection Attacks," *Proc. 2nd IEEE Int. Conf. Comput. Intell. Knowl. Econ. ICCIKE 2021*, pp. 378–383, 2021, doi: 10.1109/ICCIKE51210.2021.9410675.

[25] A. Shah, S. Clachar, M. Minimair, and D. Cook, "Building multiclass classification baselines for anomaly-based network intrusion detection systems," *Proc. - 2020 IEEE 7th Int. Conf. Data Sci. Adv. Anal. DSAA 2020*,

pp. 759–760, 2020, doi: 10.1109/DSAA49011.2020.00102.

[26] A. R. Syarif and W. Gata, “Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm,” *Proc. 11th Int. Conf. Inf. Commun. Technol. Syst. ICTS 2017*, vol. 2018-Janua, pp. 181–186, 2018, doi: 10.1109/ICTS.2017.8265667.

[27] B. Xu, S. Chen, H. Zhang, and T. Wu, “Incremental k-NN SVM method in intrusion detection,” *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, vol. 2017-Novem, pp. 712–717, 2018, doi: 10.1109/ICSESS.2017.8343013.

[28] G. Karatas, O. Demir, and O. K. Sahingoz, “Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset,” *IEEE Access*, vol. 8, pp. 32150–32162, 2020, doi: 10.1109/ACCESS.2020.2973219.

[29] A. Luo, W. Huang, and W. Fan, “A CNN-based Approach to the Detection of SQL Injection Attacks,” *Proc. - 18th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2019*, pp. 320–324, 2019, doi: 10.1109/ICIS46139.2019.8940196.

[30] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, “A detailed investigation and analysis of using machine learning techniques for intrusion detection,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 686–728, 2019, doi: 10.1109/COMST.2018.2847722.

[31] J. M. Biju, N. Gopal, and A. J. Prakash, “Cyber Attacks and Its Different Types,” *Int. Res. J. Eng. Technol.*, vol. 6, no. 3, pp. 4849–4852, 2019, [Online]. Available: https://www.irjet.net/archives/V6/i3/IRJET-V6I31244.pdf

[32] Y. Y. Aung and M. Myat Min, “Hybrid Intrusion Detection System using K-means and K-Nearest Neighbors Algorithms,” *Proc. - 17th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2018*, pp. 34–38, 2018, doi: 10.1109/ICIS.2018.8466537.

[33] Y. Xin *et al.*, “Machine Learning and Deep Learning Methods for Cybersecurity,” *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[34] Y. Liao and V. R. Vemuri, “Classifier for Intrusion,” *Comput. Secur.*, vol. 21, no. 5, pp. 439–448, 2002.

[35] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, “A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE,” *IEEE Access*, vol. 11, pp. 37131–37148, 2023, doi: 10.1109/ACCESS.2023.3266979.

[36] A. Singh, M. Singh, and K. Kumar, “A Hybrid Method for Intrusion Detection Using SVM and k-NN,” *Lect. Notes Networks Syst.*, vol. 175, no. February, pp. 119–126, 2021, doi: 10.1007/978-3-030-67187-7_13.

[37] A. R. Sonule, M. Kalla, A. Jain, and D. S. Chouhan, “Unsw-Nb15 Dataset and Machine Learning Based Intrusion Detection Systems,” *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 2638–2648, 2020, doi: 10.35940/ijeat.c5809.029320.

[38] M. Canesche, L. Bragança, O. P. V. Neto, J. A. Nacif, and R. Ferreira, “Google Colab CAD4U: Hands-on cloud laboratories for digital design,” *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2021-May, no. Vcd, 2021, doi: 10.1109/ISCAS51556.2021.9401151.

[39] I. Markoulidakis, G. Kopsiaftis, I. Rallis, and I. Georgoulas, “Multi-Class Confusion Matrix Reduction method and its application on Net Promoter Score classification problem,” *ACM Int. Conf. Proceeding Ser.*, no. Cx, pp. 412–419, 2021, doi: 10.1145/3453892.3461323.

[40] T. Kim and W. Pak, “Hybrid Classification for High-Speed and High-Accuracy Network Intrusion Detection System,” *IEEE Access*, vol. 9, pp. 83806–83817, 2021, doi: 10.1109/ACCESS.2021.3087201.