PENDEKATAN MODEL *MACHINE LEARNING* DALAM DETEKSI ANCAMAN SERANGAN SIBER DI *SECURITY OPERATION CENTER*

OLEH:

MUHAMMAD AJRAN SAPUTRA

09012682125011

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2025

PENDEKATAN MODEL *MACHINE LEARNING* DALAM DETEKSI ANCAMAN SERANGAN SIBER DI *SECURITY OPERATION CENTER*

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH:

MUHAMMAD AJRAN SAPUTRA

09012682125011

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2025

LEMBAR PENGESAHAN

PENDEKATAN MODEL *MACHINE LEARNING* DALAM DETEKSI ANCAMAN SERANGAN SIBER DI *SECURITY OPERATION CENTER*

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH:
MUHAMMAD AJRAN SAPUTRA
09012682125011

Palembang, April 2025

Pembimbing

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Mengetahui,

Koordinator Program Studi Magister Ilmu Komputer

Dr. Firdaus, M.Kom
NIP. 197801212008121003

APPROVAL SHEET

MACHINE LEARNING MODEL APPROACH IN CYBER ATTACK THREAT DETECTION IN SECURITY OPERATION CENTER

THESIS

Presented in partial fulfillment of the requirements
for the degree of Master of Computer Science

By:
MUHAMMAD AJRAN SAPUTRA
09012682125011

Palembang, April 2025

Supervisor

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Acknowledged by,

Head of Master of Computer Science Program

Dr. Firdaus, M.Kom
NIP. 197801212008121003

HALAMAN PERSETUJUAN

Pada hari Jum'at tanggal 25 April 2025 telah dilaksanakan ujian sidang tesis oleh Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Muhammad Ajran Saputra

NIM : 09012682125011

Judul : Pendekatan Model *Machine Learning* Dalam Deteksi Ancaman Serangan Siber Di *Security Operation Center*

1. **Ketua Penguji**

   Julian Supardi, S.Pd., M.T., Ph.D
   NIP. 197207102010121001 .....

2. **Penguji I**

   Dr. Ir. Ahmad Heryanto, S.Kom., M.T.
   NIP.198701222015041002 .....

3. **Penguji II**

   Hadipurnawan Satria, Ph.D
   NIP. 198004182020121001 .....

4. **Pembimbing**

   Prof. Deris Stiawan, M.T., Ph.D.
   NIP. 197806172006041002 .....

Mengetahui,
Koordinator Program Studi Magister Ilmu Komputer

Dr. Firdaus, M.Kom
NIP. 197801212008121003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Muhammad Ajran Saputra
NIM	: 09012682125011
Program Studi	: Magister Ilmu Komputer
Judul Tesis	: Pendekatan Model *Machine Learning* Dalam Deteksi Ancaman Serangan Siber Di *Security Operation Center*

Hasil Pengecekan Software iThenticate/Turnitin: **19%**

Menyatakan bahwa laporan tesis saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tesis ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, April 2025

Muhammad Ajran Saputra

NIM. 09012682125011

Machine learning model approach in cyber attack threat detection in security operation center

Muhammad Ajran Saputra

ABSTRACT

The evolution of technology roles attracted cyber security threats not only compromise stable technology but also cause significant financial loss for organizations and individuals. As a result, organizations must create and implement a comprehensive cybersecurity strategy to minimize further loss. The founding of a cybersecurity surveillance center is one of the optimal adopted strategies, known as security operation center (SOC). The strategy has become the forefront of digital systems protection. We propose strategy optimization to prevent or mitigate cyberattacks by analyzing and detecting log anomalies using machine learning models. This study employs two machine learning models: the naïve Bayes model with multinomial, Gaussian, and Bernoulli variants, and the support vector machine (SVM) model with radial basis function (RBF), linear, polynomial, and sigmoid kernel variants. The hyperparameters in both models are then optimized. The models with optimized hyperparameters are subsequently trained and tested. The experimental results indicate that the best performance is achieved by the RBF kernel SVM model, with an accuracy of 79.75%, precision of 80.8%, recall of 79.75%, and F1-score of 80.01%; and the Gaussian naïve Bayes model, with an accuracy of 70.0%, precision of 80.27%, recall of 70.0%, and F1-score of 70.66%. Overall, both models perform relatively well and are classified in the very good category (75% - 89%).

Keywords: Cyber attack, Detection, Hyperparameter, Naïve Bayes, Support vector machine

Palembang, Juni 2025

Acknowledged by,
Head of
Master of Computer Science Program

Supervisor

Dr. Firdaus, M.Kom
NIP. 197801212008121003

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

PENDEKATAN MODEL *MACHINE LEARNING* DALAM DETEKSI ANCAMAN SERANGAN SIBER DI *SECURITY OPERATION CENTER*

Muhammad Ajran Saputra

Abstrak

Evolusi peran teknologi menarik ancaman keamanan siber yang tidak hanya membahayakan teknologi yang stabil, tetapi juga menyebabkan kerugian finansial yang signifikan bagi organisasi dan individu. Oleh karena itu, organisasi harus membuat dan menerapkan strategi keamanan siber yang komprehensif untuk meminimalkan kerugian lebih lanjut. Pendirian pusat pengawasan keamanan siber adalah salah satu strategi yang diadopsi secara optimal, yang dikenal sebagai pusat operasi keamanan (SOC). Strategi ini telah menjadi yang terdepan dalam perlindungan sistem digital. Kami mengusulkan optimalisasi strategi untuk mencegah atau memitigasi serangan siber dengan menganalisis dan mendeteksi anomali log menggunakan model pembelajaran mesin. Penelitian ini menggunakan dua model pembelajaran mesin: model naïve Bayes dengan varian multinomial, Gaussian, dan Bernoulli, dan model support vector machine (SVM) dengan varian radial basis function (RBF), linear, polinomial, dan sigmoid kernel. Hyperparameter pada kedua model tersebut kemudian dioptimalkan. Model dengan hyperparameter yang telah dioptimalkan kemudian dilatih dan diuji. Hasil eksperimen menunjukkan bahwa performa terbaik dicapai oleh model SVM kernel RBF, dengan akurasi 79,75%, presisi 80,8%, recall 79,75%, dan F1-score 80,01%; dan model Gaussian naïve Bayes, dengan akurasi 70,0%, presisi 80,27%, recall 70,0%, dan F1-score 70,66%. Secara keseluruhan, kedua model memiliki kinerja yang relatif baik dan diklasifikasikan dalam kategori sangat baik (75% - 89%).

Keywords: Cyber attack, Detection, Hyperparameter, Naïve Bayes, Support vector machine

Palembang, Juni 2025

Mengetahui,
Koordinator
Program Studi Magister Ilmu Komputer

Dr. Firdaus, M.Kom
NIP. 197801212008121003

Pembimbing

Prof. Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT karena atas rahmat-Nya penulis dapat menyelesaikan laporan tesis ini. Tesis yang berjudul "**Pendekatan Model *Machine Learning* Dalam Deteksi Ancaman Serangan Siber Di *Security Operation Center***" ini disusun untuk memperoleh gelar magister pada Program Studi Magister Ilmu Komputer Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah membantu untuk menyelesaikan tesis ini, yaitu kepada:

1. Kedua orang tua serta Saudara-saudariku atas semua bantuan yang tak dapat penulis hitung dan tuliskan satu persatu;
2. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya;
3. Bapak Dr. Firdaus, M.Kom. selaku Ketua Program Studi Magister Ilmu Komputer.
4. Bapak Prof. Ir. Deris Stiawan, M.T., Ph.D, selaku pembimbing yang telah banyak memberikan bimbingan, masukan dan bantuan dalam proses penyelesaian tesis ini;
5. Ibu Fariza Musfa Safina, S.E. selaku istri penulis yang membersamai penulis dalam keadaan suka & duka.
6. Bapak dan Ibu Dosen yang selama ini telah melimpahkan ilmunya kepada penulis selama proses belajar mengajar di Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Kak Abdi selaku Admin Prodi Magister Ilmu Komputer UNSRI, yang telah membantu penulis dalam menyelesaikan penulisan thesis.
8. Kelompok Riset bidang jaringan komputer, enterperise dan keamanan informasi Universitas Sriwijaya (COMNETS RG)
9. Seluruh teman-teman mahasiswa Magister Ilmu Komputer dan seluruh teman-teman akademika Fakultas Ilmu Komputer.
10. Untuk semua pihak yang telah membantu dalam penyelesaian tugas akhir ini dan tidak dapat disebutkan satu-persatu.

Akhir kata, penulis menyadari bahwa tesis ini jauh dari kata sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun dari semua pihak untuk penyempurnaan laporan tesis ini dan semoga tesis ini dapat bermanfaat bagi pihak yang membutuhkan.

Palembang, Mei 2025

Penulis

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang dilakukannya penelitian yang berjudul Pendekatan Model *Machine Learning* Dalam Deteksi Ancaman Serangan Siber di *Security Operation Center* (SOC). Pada sub-bab selanjutnya, dari latar belakang tersebut dapat dirumuskan permasalahan yang akan dibahas, agar permasalahan tidak meluas maka diberikan batasan masalah. Kemudian, dirumuskan tujuan dan manfaat dari penelitian yang dibuat, dan sistematika yang digunakan dalam penelitian tersebut.

1.1 Latar Belakang Masalah

Traffic Anomaly adalah keadaan tidak stabil dalam lalu lintas jaringan yang dapat membuat jaringan rentan terhadap serangan. Selain itu, *Traffic Anomaly* atau Anomali Lalu Lintas juga dapat melumpuhkan jaringan dari sisi file yang menjadi target penyusup (Riadi, et al., 2019). Menurut laporan Badan Siber dan Sandi Negara RI, pada bulan Maret 2025 terdapat *Traffic Anomaly* yang masuk ke Indonesia mencapai 15.895.675 anomali trafik. Klasifikasi menunjukkan bahwa hampir 50% dari total trafik tersebut terindikasi sebagai serangan malware dan trojan (BADAN SIBER DAN SANDI NEGARA RI, 2025).

Dalam mengatasi atau mencegah anomali lalu lintas, terdapat beberapa cara, salah satunya adalah melakukan analisis dan deteksi anomali log, deteksi anomali lalu lintas jaringan dapat membantu mendeteksi lalu lintas data yang tidak normal di jaringan, mengidentifikasi pola atau perilaku yang tidak biasa dalam lalu lintas jaringan, menentukan potensi ancaman keamanan, dan memungkinkan tindakan penanggulangan yang tepat waktu. Deteksi anomali lalu lintas jaringan merupakan area penting dari keamanan jaringan, dan merancang serta memilih metode yang tepat dapat meningkatkan keamanan jaringan (Zhao, et al., 2024). Deteksi anomali dapat dilakukan dengan cara memeriksa log secara manual, tetapi pendekatan ini tidak praktis karena kompleksitas dan besarnya jumlah data yang ada (Shah, et al., 2022). Deteksi anomali sangat penting karena data yang terdeteksi dapat mewakili informasi yang signifikan, kritis, dan dapat ditindaklanjuti (Nassif, et al., 2021).

Maka dari itu, diperlukan proses otomatis untuk menganalisis dan mengklasifikasikan log terkait anomali lalu lintas (Shah, et al., 2022).

Salah satu sistem yang menganalisis dan mengklasifikasikan log terkait anomali lalu lintas menggunakan metode *machine learning*. Metode *machine learning* telah menjadi teknik yang efektif untuk mengidentifikasi dan mengategorikan berbagai jenis serangan jaringan atau serangan siber (Situmorang, 2023). Penelitian sebelumnya yang menerapkan metode *machine learning* untuk deteksi serangan siber dilakukan oleh (Veena, et al., 2022) yang membahas perbandingan SVM dan KNN dalam mendeteksi kejahatan siber. Penelitian tersebut menggunakan dataset dari Ecml-Pkdd 2007 yang berisi data kejahatan siber dalam sektor perbankan. Hasil penelitian menunjukkan bahwa SVM memiliki akurasi tertinggi sebesar 98,8%, dibandingkan dengan KNN yang memiliki akurasi sebesar 96,47%. Penelitian lainnya dilakukan oleh (Vishwakarma & Kesswani, 2023) yang membahas tentang Intrusion Detection System dengan membandingkan algoritma Naive Bayes dengan algoritma Logistic Regression, KNN, Decision Tree, Random Forest, LDA, QDA, AdaBoost, Gradient Boosting, dan Extra Trees. Penelitian ini menggunakan dua jenis dataset, yaitu NSL-KDD dan UNSW_NB15. Hasil penelitian menunjukkan bahwa Naive Bayes menghasilkan performa terbaik dengan akurasi tertinggi pada dataset NSL-KDD sebesar 97,1% dan pada dataset UNSW_NB15 sebesar 86,9%.

Oleh karena itu, dalam penelitian ini, untuk mengurangi beban kerja *Security Operation Center* (SOC), akan dilakukan analisis dan klasifikasi serangan siber terhadap log sistem berbasis AI dengan membandingkan algoritma *Naive Bayes* dan *Support Vector Machine* (SVM). Penggunaan *Naive Bayes* dalam penelitian ini dikarenakan algoritma tersebut memiliki kelebihan, yaitu cocok diterapkan pada data dalam jumlah besar dan mampu menangani data yang kosong (*missing value*) (Arifin & Ariesta, 2019). Penggunaan SVM dalam penelitian ini dipilih karena SVM merupakan model machine learning yang dapat digunakan untuk masalah klasifikasi maupun regresi. Selain itu, algoritma SVM bekerja dengan baik di ruang berdimensi tinggi atau dalam situasi di mana jumlah dimensi melebihi jumlah sampel (Chhajer, et al., 2022). Dengan adanya penelitian ini, diharapkan dapat

melakukan deteksi ancaman serangan siber dengan memanfaatkan data log sistem berbasis AI melalui perbandingan algoritma SVM dan *Naive Bayes*.

1.2 Rumusan Masalah

Berdasarkan latar belakang dan kesenjangan yang diidentifikasi dari kondisi saat ini, penulis merumuskan permasalahan terkait solusi untuk melakukan deteksi ancaman serangan siber di Security Operation Center (SOC). Selanjutnya, pertanyaan utama tersebut akan dijabarkan secara lebih mendetail sebagai berikut:

1. Bagaimana melakukan deteksi ancaman serangan siber di *Security Operation Center* (SOC) menggunakan data log sistem berbasis AI?
2. Bagaimana melakukan pendekatan model *machine learning* dalam mendeteksi ancaman serangan siber di *Security Operation Center* (SOC) menggunakan data log sistem berbasis AI?
3. Bagaimana performa model *Machine Learning Naive Bayes* dan *Support Vector Machine* dalam mendeteksi ancaman serangan siber di *Security Operation Center* (SOC) menggunakan log sistem berbasis AI*?*

1.3 Batasan Masalah

Batasan dalam melakukan proses deteksi anomali yang dirancang pada thesis ini adalah :

1. Dataset yang digunakan berasal dari Loghub menggunakan dataset Hadoop.
2. Pembobotan dilakukan menggunakan TF-IDF.
3. Algoritma yang digunakan dalam melakukan klasifikasi yaitu algoritma *Naive Bayes* dan *Support Vector Machine*.
4. Jenis metode *naive bayes* yang digunakan yaitu *Naïve Bayes Gaussian, Naïve Bayes Bernoulli* dan *Naïve Bayes Multinomial.*
5. Kernel *Support Vector Machine* yang digunakan yaitu *Radial Bias Function* (RBF), *linear, polynomial* dan *sigmoid.*
6. *Output* penelitian ini berupa klasifikasi ancaman serangan siber dalam log sistem menggunakan model *machine learning Naive Bayes* dan *Support Vector Machine.*

1.4 Tujuan

Adapun tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut:

1. Melakukan deteksi terhadap ancaman serangan siber di *Security Operation Center* (SOC) menggunakan data log sistem berbasis AI.
2. Melakukan pendekatan model *machine learning* dalam mendeteksi ancaman serangan siber di *Security Operation Center* (SOC) menggunakan data log sistem berbasis AI.
3. Mengetahui performa model *machine learning Naive Bayes* dan *Support Vector Machine* dalam mendeteksi ancaman serangan siber di *Security Operation Center* (SOC) menggunakan log sistem berbasis AI.

1.5 Manfaat

Sedangkan, manfaat yang dapat diambil dari penelitian ini adalah:

1. Memberikan kontribusi untuk penelitian deteksi anomali menggunakan *machine learning.*
2. Memudahkan pemahaman terhadap setiap ancaman yang mungkin terjadi pada *log files.*
3. Hasil dari penelitian dapat menjadi referensi untuk penelitian dibidang deteksi anomali menggunakan *machine learning*.

1.6 Sistematika Penulisan

Untuk memudahkan penyusunan proposal tesis ini dan memperjelas isi setiap bab dalam laporan ini, dibuatlah sistematika penulisan sebagai berikut:

1. **BAB I Pendahuluan**

   Bab ini berisi latar belakang yang menjelaskan alasan mengapa penelitian ini penting, serta mencakup rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan.

2. **BAB II Tinjauan Pustaka**

   Bab ini menyajikan penjelasan menyeluruh mengenai tinjauan pustaka yang relevan dengan masalah yang dibahas dalam penelitian ini.

3. **BAB III** **Metodologi Penelitian**

   Bab ini berisi alasan dan metode penelitian, data yang digunakan, metode analisis, serta analisis hasil. Hal ini disusun untuk membentuk kerangka penelitian dalam pelaksanaan penelitian ini.

4. **BAB IV** **Hasil dan Analisis**

   Bab ini berisi hasil dan analisis terhadap hasil pengerjaan tesis yang telah dilakukan.

5. **BAB V** **Kesimpulan dan Saran**

   Bab ini berisi kesimpulan dari hasil yang telah diperoleh dari pengerjaan tesis. Selain itu, bab ini juga memuat saran dan kekurangan yang mungkin dapat dikembangkan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Agarwal, A., Sharma, P. & Alshehri, M., 2021. Classification model for accuracy and intrusion detection using machine learning approach. *PeerJ Computer Science*, pp. 1-22.

Akanle, M. et al., 2020. Experimentations with OpenStack System Logs and Support Vector Machine for an Anomaly Detection Model in a Private Cloud Infrastructure. *IEEE.*

Al-amri, R., Murugesan, R. K., Man, M. & Abdulateef, A. F., 2021. A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. *applied sciences*, pp. 1-23.

Angkasa, V. & Pangaribuan, J. J., 2022. Komparasi Tingkat Akurasi Random Forest Dan Knn Untuk Mendiagnosis Penyakit Kanker Payudar. *Information System Development,* Volume 10, pp. 34-41.

Arifin, T. & Ariesta, D., 2019. Prediksi Penyakit Ginjal Kronis Menggunakan Algoritma Naive Bayes Classifier Berbasis Particle Swarm Optimization. *Jurnal Tekno Insentif,* Volume 13, pp. 26-30.

Basar, T. F., Ratnawati, D. E. & Arwani, I., 2022. Analisis Sentimen Pengguna Twitter terhadap Pembayaran Cashless menggunakan Shopeepay dengan Algoritma Random Forest. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, pp. 1426-1433.

Chhajer, P., Shah, M. & Kshirsagar, A., 2022. The applications of artificial neural networks, support vector machines, and long–short term memory for stock market prediction. *Decision Analytics Journal*, pp. 1-12.

Devi, R. & Badugu, S., 2021. Network Intrusion Detection System Using KNN and Naive Bayes Classifiers. *Turkish Online Journal of Qualitative Inquiry (TOJQI),* pp. 8226-8235.

Fajri, F. N., Tholib, A. & Yuliana, W., 2022. Penerapan Machine Learninguntuk Penentuan Matakuliah Pilihan pada Program Studi Informatika. *Jurnal Teknik Informatika dan Sistem Informasi.*

Fathurohman, A., 2021. Machine Learninguntuk Pendidikan:Mengapa Dan Bagaimana. *Jurnal Informatika Dan Teknologi Komputer.*

Firmansyach, W. A., Hayati, U. & Wijaya, Y. A., 2023. Analisa Terjadinya Overfitting dan Underfitting pada Algoritma Naive Bayes dan Decision Tree dengan Teknik Cross Validation. *JATI: Jurnal Mahasiswa Teknik Informatika*, Volume 7, pp. 262-269.

Hermawan, E., Agustian, S. & Saputra, D. M., 2023. Klasifikasi Kesehatan Pada Tanaman Padi Menggunakan Citra Unmaned Aerial Vehicle (UAV) Dengan Metode Convolutional Neural Networks (CNN). *Jurnal Ilmiah Teknologi Informasi Terapan,* Volume 9, pp. 308-318.

Ibrahim, H., Anwar, S. A. & Ahmad, M. I., 2020. Classification of imbalanced data using support vector machine and rough set theory: A review. *Journal of Physics: Conference Series,* pp. 1-12.

Luan, Y. & Lin, S., 2019. Research on Text Classification Based on CNN and LSTM. *IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) ,* pp. 352-355.

Naji, M. A. et al., 2021. Machine Learning Algorithms For Breast Cancer Prediction and Diagnosis. *Procedia Computer Science*, pp. 487-492.

Nassif, A. B., Talib, M. A., Nasir, Q. & Dakalbab, F. M., 2021. Machine Learning for Anomaly Detection: A Systematic Review. *IEEEAccess.*

Nooraeni, R. et al., 2020. Analisis Sentimen Data Twitter Mengenai Isu RUU KPK Dengan Metode Support Vector Machine (SVM). *Paradigma - Jurnal Informatika dan Komputer,* pp. 55-60.

Novianti, D., 2019. Implementasi Algoritma Naive Bayes pada Data Set Hepatitis Menggunakan Rapid Miner. *Jurnal Komputer dan Informatika Akademi Bina Saran Informatika*, Volume 21, pp. 49-54.

Nurdin, M., Asmawati, A. & Najamuddin, M., 2023. Investigating the Effect of Using English Islamic Pop Songs on Students' Vocabulary Size. *Indonesian Tesol Journal*, Volume 5, pp. 272-283.

Pamungkas, T. J. & Romadhony, A., 2021. Analisis Sentimen Berbasis Aspek Terhadap Ulasan Restoran Berbahasa Indonesia Menggunakan Support Vector Machines. *e-Proceeding of Engineering* , 8(4), pp. 4102-4114.

Praghakusma, A. Z. & Charibaldi, N., 2021. Komparasi Fungsi Kernel Metode Support Vector Machine untuk Analisis Sentimen Instagram dan Twitter (Studi Kasus : Komisi Pemberantasan Korupsi). *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal),* p. 88.

Pratama, H. K. C. A., Suharso, W. & A'yun, Q., 2022. Pengklasifikasian Kanker Payudara dan Kanker Paru-Paru dengan Metode Gaussian Naive Bayes, Multinomial Naive Bayes. dan Bernoulli Naive Bayes. *Jurnal Smart Teknologi,* pp. 350-355.

Pratama, R. R., 2020. Analisis Model Machine Learning Terhadap Pengenalan Aktifitas Manusia. *Jurnal MATRIK,* pp. 302-311.

Pravina, A. M., Cholissodin, I. & Adikara, P. P., 2019. Analisis Sentimen Tentang Opini Maskapai Penerbangan pada Dokumen Twitter Menggunakan Algoritme Support Vector Machine (SVM). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* pp. 2789-2797.

Que, V. K. S., Iriani, A. & Purnomo, H. D., 2020. Analisis Sentimen Transportasi Online Menggunakan Support Vector Machine Berbasis Particle Swarm Optimization. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 9(2), pp. 162-170.

Rahman, M., Islam, D., Mukti, R. J. & Saha, I., 2020. A deep learning approach based on convolutional LSTM for detecting. *Computational Biology and Chemistry,* pp. 1-10.

Riadi, I., Umar, R. & Aini, F. D., 2019. Analisis Perbandingan Detection Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector Machine (SVM). *ILKOM Jurnal Ilmiah* , pp. 11(1), 17-24.

Ryciak, P., Wasielewska, K. & Janicki, A., 2022. Anomaly Detection in Log Files Using Selected Natural Anomaly Detection in Log Files Using Selected Natural. *applied scinences,* pp. 1-16.

Shah, A. H., Pasha, D., Zadeh, E. H. & Konur, S., 2022. Automated Log Analysis and Anomaly Detection Using Machine Learning. *IOS Press.*

Shin, Y. & Kim, K., 2020. Comparison of Anomaly Detection Accuracy of Host-based Intrusion Detection. *(IJACSA) International Journal of Advanced Computer Science and Applications*, pp. 252-259.

Situmorang, S., 2023 . Analisis Kinerja Algoritma Machine Learning Dalam Deteksi Anomali Jaringan. *Konstanta : Jurnal Matematika dan Ilmu Pengetahuan Alam*, Volume 1, pp. 258-269.

Veena, K. et al., 2022. SVM Classification and KNN Techniques for Cyber. *Hindawi*, pp. 1-9.

Vishwakarma, M. & Kesswani, N., 2023. A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection. *Decision Analytics Journal.*

Zhao, Z., Guo, H. & Wang, Y., 2024. A multi-information fusion anomaly detection model based on convolutional neural networks andAutoEncoder. *Scientifc Report*, Volume 14.

Zhu, J. et al., 2023. Loghub: A Large Collection of System Log Datasets for AI-driven Log Analytics. *arxiv*, pp. 1-12.