PENERAPAN METODE *EXTREME GRADIENT BOOSTING* UNTUK DETEKSI *MULTI-CLASSIFICATION* SERANGAN SIBER

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer

OLEH:

Edwar Azy Sangsoko

09011382126160

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

PENERAPAN METODE EXREME GRADIENT BOOSTING UNTUK DETEKSI MULTI-CLASSFIFCATION SERANGAN SIBER

Sebagai salah satu syarat untuk penyelesaian studi di
Program Studi S1 Sistem Komputer

Oleh:

EDWAR AZY SANGSOKO

09011382126160

Pembimbing 1 : Dr. Ahmad Heryanto, S.kom., M.T.

NIP. 198701222015041002

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

199612032006041001

AUTHENTICATION PAGE

FINAL TASK

IMPLEMENTATION OF EXTREME GRADIENT BOOSTING METHOD FOR MULTI-CLASSIFICATION DETECTION OF CYBER ATTACKS

Submited to Complete One of the Requirements for Obtaining a Bachelor's Degree in Computer Science

By:

EDWAR AZY SANGSOKO

09011382126160

Supervisor 1 : **Dr. Ahmad Heryanto, S.kom., M.T.**

NIP. 198701222015041002

Acknowledge,

Head of Computer System Department

Dr. Ir. Sukemi, M.T.

199612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : **Kamis**

Tanggal : **24 Juli 2025**

1. **Ketua** : **Huda Ubaya, M. T.**

2. **Pembimbing** : **Dr. Ir. Ahmad Heryanto, M.T.**

3. **Penguji** : **Yoppy Sazaki, S.Si., M.T.**

Mengetahui, 17/9/25

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

199612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Edwar Azy Sangsoko

Nim : 09011382126160

Judul : Penerapan Metode *Extreme Gradient Boosting* untuk Deteksi *Multi-Classification* Serangan Siber.

Hasil pengecekan *Software Turnitin*: 1%

Menyatakan bahwa Laporan Tugas Akhir saya merupakan hasil karya sendiri bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam Laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, September 2025

Penulis,

Edwar Azy Sangsoko

NIM. 09011382126160

KATA PENGANTAR

Puji Syukur penulis panjatkan kehadirat Allah swt. atas limpahan rahmat dan karunianya, sehingga penulis dapat menyelesaikan penyusunan Laporan Tugas Akhir ini yang berjudul "**Penerapan Metode Extreme Gradient Boosting Untuk Deteksi Multi-Classification Serangan Siber**".

Penyusunan Laporan Tugas Akhir ini tidak terlepas dari peran serta beberapa pihak yang telah membantu, memberikan motivasi, kemudahan, pengarahan, bimbingan, dorongan semangat, kritik dan sara dengan hati yang tulus dan penuh keihklasan selama proses penyusunan Tugas Akhir ini. Penulis ingin menyampaikan rasa syukur dan terimakasih serta penghargaan yang tak terhingga sedalam-dalamnya kepada:

1. Allah SWT. yang telah memberikan kesehatan, kemudahan, serta keberkahan sehingga penulis dapat menyelesaikan kerja praktik beserta laporannya dengan baik.
2. Orang tua penulis yang telah membesarkan saya dengan penuh kasih sayang dan telah banyak memberikan do'a serta dukungan dan semangat kepada penulis dalam menyelesaikan pengerjaan Tugas Akhir.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Dr. Rossi Passarella., M.Eng., selaku Dosen Pembimbing Akademik yang telah berkenan memberikan saran dan arahan untuk penulis dalam menyiapkan Tugas Akhir.
6. Bapak Dr. Ir. Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan tugas akhir ini.
7. Mbak Sari dan Mbak Titi selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.

8. Kepada teman seperjuangan penulis saudara Ahmed Athalla Toyyib, Farel Firjatullah, Jonathan Samuel dan seluruh teman teman Jurusan Sistem Komputer Angkatan 2021 yang telah membantu saya dalam memberi semangat dalam penulisan tugas akhir ini.
9. Dan semua pihak yang telah membantu dalam penyelesaian tugas akhir ini dan tidak dapat disebutkan satu-persatu.

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.

Palembang, September 2025

Penulis,

Edwar Azy Sangsoko

NIM. 09011382126160

PENERAPAN METODE *EXTREME GRADIENT BOOSTING* UNTUK DETEKSI *MULTI-CLASSIFICATION* SERANGAN SIBER

Edwar Azy Sangsoko (09011382126160)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: edwarazy1703@gmail.com

ABSTRAK

Dalam era digital yang berkembang, ancaman keamanan siber semakin meningkat. Salah satu solusi yang umum digunakan dalam mengamankan jaringan adalah Network Intrusion Detection System (NIDS). Untuk meningkatkan kinerja NIDS penelitian ini menerapkan metode Machine Learning (ML) yaitu metode Extreme Gradient Boosting (XGBoost), karena dipertimbangkan memiliki performanya yang tinggi dan kemampuannya dalam menangani data yang kompleks dan tidak seimbang. Sehingga penelitian ini bertujuan untuk mengevaluasi kinerja algoritma XGBoost dalam mendeteksi berbagai jenis serangan siber menggunakan lima dataset benchmark yang umum digunakan pada sistem deteksi intrusi, yaitu NSL-KDD, UNSW-NB15, CIC-IDS2017, CSE-CIC-IDS2018, dan ToN-IoT. Dalam penelitian ini, XGBoost digunakan sebagai algoritma utama untuk mendeteksi dan mengklasifikasikan berbagai jenis serangan siber dalam bentuk multi-class classification. Oleh karena itu, dalam penelitian ini memiliki tahapan pra-pemrosesan, seleksi fitur, dan optimasi hyperparameter tuning. Serta, digunakan beberapa metrik evaluasi utama seperti akurasi, precision, recall, F1-score, confusion matrix, dan ROC-AUC.

Kata Kunci: Network Intrusion Detection System (NIDS), Machine Learning (ML), Extreme Gradient Boosting (XGBoost), Klasifikasi Multikelas, Hyperparameter Tuning.

IMPLEMENTATION OF EXTREME GRADIENT BOOSTING METHOD FOR MULTI-CLASSIFICATION DETECTION OF CYBER ATTACKS

Edwar Azy Sangsoko (09011382126160)
Department of Computer Systems, Faculty of Computer Science,
Sriwijaya University
Email: edwarazy1703@gmail.com

ABSTRACT

In the developing digital era, cybersecurity threats are increasing. One of the solutions commonly used in securing networks is the Network Intrusion Detection System (NIDS). To improve the performance of NIDS, this study applies the Machine Learning (ML) method, namely the Extreme Gradient Boosting (XGBoost) method, because it is considered to have high performance and its ability to handle complex and imbalanced data. Therefore, this study aims to evaluate the performance of the XGBoost algorithm in detecting various types of cyber attacks using five benchmark datasets commonly used in intrusion detection systems, namely NSL-KDD, UNSW-NB15, CIC-IDS2017, CSE-CIC-IDS2018, and ToN-IoT. In this study, XGBoost is used as the main algorithm to detect and classify various types of cyber attacks in the form of multi-class classification. Therefore, in this study has stages of pre-processing, feature selection, and hyperparameter tuning optimization. Also, several main evaluation metrics are used such as accuracy, precision, recall, F1-score, confusion matrix, and ROC-AUC.

Keywords: Network Intrusion Detection System (NIDS), Machine Learning (ML), Extreme Gradient Boosting (XGBoost), multi-class classification, Hyperparameter Tuning.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Selama beberapa tahun terakhir, internet telah berkembang menjadi pusat bagi berbagai aktivitas dan transaksi yang terjadi di jaringan global, termasuk yang bersifat bisnis, sosial, politik, dan lainnya. Pengguna yang menjadi titik akhir dari transaksi jaringan tersebut biasanya berada dalam jaringan komputer yang lebih kecil, seperti perusahaan atau sub-jaringan penyedia layanan internet skala kecil. Oleh karena itu, keamanan telah menjadi isu penting bagi pengguna internet modern, meskipun berbagai solusi deteksi intrusi telah ada selama hampir 40 tahun [1].

Ancaman kini semakin beragam, mulai dari Distributed Denial-of-Service (DDoS), ransomware, Advanced Persistent Threats (APTs), viruses, worms, malware, spyware, botnets, spam, spoofing, phishing, hacktivism, hingga potensi serangan siber yang disponsori negara. Data tahun 2019 menunjukkan 1.272 pelanggaran dengan hampir 163 juta data terekspos, rata-rata 128.171 data per insiden, dengan sektor perbankan mencatat jumlah pelanggaran tertinggi dan sektor kesehatan mengalami persentase terbesar dari kebocoran data sensitif. Serangan DDoS menjadi ancaman dominan bagi penyedia layanan, dengan penyerang memanfaatkan kerentanan jaringan dan infrastruktur untuk melumpuhkan sistem, sehingga memaksa penyedia keamanan berupaya membuat serangan ini tidak lagi menguntungkan secara finansial bagi pelaku [2].

Jumlah penyerang telah meningkat sebagai akibat dari kemajuan teknologi informasi. Serangan awal terutama dilakukan untuk kesenangan dan minat teknologi. Namun, serangan tersebut meningkat secara eksplosif dalam beberapa tahun terakhir, menyebabkan kerugian finansial yang signifikan bagi organisasi yang berbasis jaringan komputer. Untuk memerangi kejahatan dunia maya, strategi yang efektif harus dikembangkan dan diterapkan. Menerapkan *Network Intrusion Detection System* (NIDS) yang efektif adalah masalah utama dalam keamanan jaringan [3].

NIDS memiliki kemampuan untuk melacak dan mengidentifikasi serangan berbahaya tersebut dengan memantau lalu lintas jaringan dan menemukan pola mencurigakan pada paket masuk dan keluar, serta lalu lintas jaringan lokal. NIDS berbasis *signature* (pola tanda serangan) dan *anomaly* (anomali / penyimpangan). Skema deteksi berbasis anomali melihat apakah perilaku jaringan menyimpang dari perilaku normal dengan menganalisis lalu lintas jaringan untuk *byte* (bit) data atau rangkaian paket yang diketahui menunjukkan anomali. Namun, serangan berbasis *signature* tidak dapat mendeteksi serangan yang tidak diketahui, jadi *anomaly detection* NIDS lebih baik ketika mencoba mengidentifikasi serangan berbasis *signature* yang tidak diketahui [4].

Saat ini, teknik deteksi anomali jaringan biasanya menggunakan model *machine learning* (ML), seperti *K-nearest neighbor* (KNN) dan *Support Vector Machine* (SVM). Meskipun metode ini bekerja dengan baik, itu tidak begitu akurat [5]. Dalam beberapa tahun terakhir, teknik ML telah menjadi lebih populer, seperti dalam menemukan tindakan normal pada awal pencarian aktivitas berbahaya di sistem komputer. Akibatnya, mereka dapat melindungi pengguna dengan menjaga keamanan sistem dan menghentikan serangan lebih cepat dari sebelumnya. *AdaBoost* [6], *Naïve Bayes* (NB) dan *Random Forest* (RF) [7], Selain metode umum seperti *Logistic Regression* (LR) dan SVM [8], algoritma baru untuk meningkatkan kinerja seperti XGBoost telah diusulkan [9].

Dengan kemampuan paralel yang sederhana dan prediksi dengan tingkat akurasi yang tinggi, algoritma *Extreme Gradient Boosting*, atau XGBoost, adalah salah satu alat yang paling kompetitif dan andal dalam metode kecerdasan buatan saat ini [10]. XGBoost adalah implementasi *Gradient Boosting Machine* (GBM) yang dirancang untuk efisiensi dan skalabilitas tinggi. Algoritma ini menggunakan pohon keputusan sebagai pengklasifikasi utamanya dan menerapkan fungsi kerugian baru untuk mengendalikan kompleksitas pohon. Dalam proses optimasi bertahap, XGBoost mempertahankan hasil perhitungan sebelumnya untuk digunakan oleh pengklasifikasi berikutnya. Pendekatan ini, yang dikenal sebagai regularisasi, membantu meningkatkan efisiensi dan akurasi model XGBoost [11].

Berdasarkan penelitian [12], model IDS berbasis XGBoost dengan seleksi fitur dan kombinasi teknik *deep learning* seperti BiLSTM, ANN, dan 1D-CNN telah menunjukkan hasil yang sangat baik dalam mengklasifikasikan serangan siber. Penelitian ini

mengimplementasikan teknik *balancing* (menyeimbangkan) data menggunakan SMOTE untuk mengatasi ketidakseimbangan kelas pada dataset seperti NSL-KDD, CIC-IDS2017, dan UNSW-NB15. Hasilnya, model yang diusulkan mencapai akurasi hingga 99% dan peningkatan signifikan dalam precision(presisi/ ketepatan) dan recall (sensitivitas/ cakupan), khususnya untuk kelas serangan yang jarang. Kesimpulan penelitian ini menegaskan bahwa kombinasi XGBoost untuk seleksi fitur dan arsitektur *deep learning* dengan *balancing* data dapat meningkatkan efektivitas deteksi serangan, serta direkomendasikan untuk diterapkan pada dataset yang lebih luas atau eksplorasi lebih lanjut untuk memperkuat keamanan siber.

Pada penelitian [13], bahwa model XGBoost terbukti efektif untuk digunakan dalam IDS dengan memanfaatkan dataset NSL-KDD. Model ini menunjukkan kemampuan klasifikasi yang unggul dengan tingkat akurasi yang mencapai 98,7%, *precision* sebesar 98,41%, *recall* 99,11%, dan *F1-score* 98,76%. Penggunaan XGBoost memberikan keunggulan berupa pengurangan *overfitting* (kelebihan pelatihan) melalui regularisasi, fleksibilitas dalam pengaturan parameter, serta kemampuan memproses data secara efisien. Selain itu, pemanfaatan *confusion matrix* dan *ROC curve* membantu mengevaluasi kinerja model secara komprehensif. Penelitian ini memberikan landasan yang kuat untuk pengembangan IDS yang lebih baik dan aman, dengan peluang untuk menerapkan optimasi lebih lanjut atau memperluas model ini ke klasifikasi multikelas di masa depan.

Algoritma XGBoost diterapkan pada penelitian [14], membangun model deteksi intrusi berbasis pembelajaran mesin menggunakan dataset CICIDS2017. Dengan melalui tahapan *pre-processing* (pra-pemrosesan), seleksi fitur berdasarkan *feature importance* (fitur yang paling berpengaruh), dan *tuning parameter* (penyetelan/pengaturan parameter), model ini mampu mengidentifikasi intrusi secara efektif dengan rata-rata akurasi 98%, precision 0.98, recall 0.98, F1-score 0.98, dan AUC 0.99. Hasil ini menunjukkan bahwa pendekatan berbasis XGBoost tidak hanya memberikan performa yang menjanjikan tetapi juga unggul dibandingkan studi serupa. Dengan pemrosesan semua subset dataset, penelitian ini menunjukkan pendekatan menyeluruh yang meningkatkan efisiensi dan generalisasi model untuk berbagai jenis serangan siber.

Berdasarkan pembahasan yang telah diuraikan, penulis tertarik memilih judul **"PENERAPAN METODE *EXTREME GRADIENT BOOSTING* UNTUK DETEKSI**

***MULTI-CLASSIFICATION* SERANGAN SIBER"**. Penelitian ini menggunakan dataset serangan siber sebagai bahan analisis untuk menguji efektivitas XGBoost dalam mengklasifikasikan berbagai jenis serangan. Metode XGBoost dipilih karena kemampuannya dalam menangani kompleksitas data, melakukan seleksi fitur secara otomatis, dan mengatasi ketidakseimbangan kelas, sehingga diharapkan dapat memberikan hasil deteksi yang lebih akurat dan efisien.

1.2 Rumusan Masalah

Berdasarakan latar belakang di atas, peneliti merumuskan masalah yaitu sebagai berikut:

1. Bagaimana penerapan metode Extreme Gradient Boosting (XGBoost) dalam mendeteksi serangan siber dengan pendekatan multi-classification?
2. Bagaimana performa model XGBoost bervariasi pada beberapa dataset serangan siber?
3. Bagaimana akurasi dan efektivitas metode XGBoost dibandingkan dengan metode lainnya dalam mendeteksi berbagai jenis serangan siber?

1.3 Tujuan

Berdasarkan rumusan masalah di atas, penelitian ini memiliki beberapa tujuan yang harus dicapai yaitu:

1. Menerapkan metode Extreme Gradient Boosting (XGBoost) untuk mendeteksi berbagai jenis serangan siber dengan pendekatan multi-classification.
2. Untuk mengevaluasi kinerja model XGBoost dalam mendeteksi serangan siber pada berbagai dataset serangan siber, seperti NSL-KDD, UNSW-NB15, CIC-IDS2018, dan lainnya.
3. Membandingkan akurasi dan efektivitas XGBoost dengan metode lainnya, seperti algoritma deep learning atau machine learning tradisional, dalam mendeteksi berbagai tipe serangan siber.

1.4 Manfaat

Berdasarkan tujuan dari penelitian ini, memiliki beberapa manfaat antara lain sebagai berikut:

1. Penelitian ini membantu mengembangkan metode deteksi serangan siber yang lebih efektif dan akurat melalui penerapan algoritma XGBoost, termasuk pada serangan multi-klasifikasi.
2. Memberikan gambaran dan evaluasi kinerja XGBoost sebagai salah satu algoritma pembelajaran mesin yang dapat diandalkan dalam mendeteksi serangan siber secara otomatis.
3. Dengan membandingkan XGBoost dengan metode deep learning dan machine learning tradisional, penelitian ini memberikan dasar yang kuat untuk memilih metode deteksi yang paling sesuai berdasarkan jenis ancaman dan kebutuhan sistem.

1.5 Batasan Masalah

Dalam penelitian yang dilakukan terdapat beberapa batasan masalah, yaitu :

1. Penelitian ini menggunakan dataset UNSW-NB15, CIC-IDS2018, CIC-IDS2017, NSL-KDD, TON_IoT sebagai sumber data untuk pelatihan dan pengujian model deteksi serangan siber. Dataset ini dipilih karena mencakup berbagai jenis serangan siber dalam skenario multi-klasifikasi.
2. Algoritma utama yang digunakan dalam penelitian ini adalah Extreme Gradient Boosting (XGBoost). Model lain hanya digunakan untuk keperluan perbandingan kinerja.
3. Penelitian ini dilakukan dalam lingkungan simulasi berbasis perangkat lunak menggunakan bahasa pemrograman Python dan pustaka terkait seperti XGBoost.
4. Proses preprocessing mencakup teknik standar seperti pembersihan data, transformasi data, dan feature selection. Teknik lain yang lebih kompleks tidak menjadi fokus utama.

1.6 Metode Penelitian

Metode penelitian yang akan digunakan pada penelitian ini sebagai berikut:

1. Tahap Pertama (Identifikasi Masalah)

Mengidentifikasi tantangan utama dalam mendeteksi serangan siber, terutama dalam skenario multi-klasifikasi, seperti masalah akurasi, dan kebutuhan akan model yang efisien.

2. Tahap Kedua (Studi Literatur)

   Melakukan kajian pustaka untuk memahami konsep dasar intrusion detection system (IDS), serangan siber, algoritma Extreme Gradient Boosting (XGBoost). Kemudian, mencari beberapa sumber seperti artikel, jurnal buku, internet dan sumber-sumber lainnya yang berhubungan dengan proposal ini.

3. Tahap Ketiga (Pengumpulan Data)

   Dataset yang digunakan adalah UNSW_NB15, CIC-IDS2018, CIC-IDS2017, NSL-KDD, TON_IoT yang mencakup berbagai jenis serangan siber dan trafik jaringan normal. Dataset ini diperoleh dari sumber terpercaya untuk keperluan penelitian IDS.

4. Tahap Keempat (Pengembangan Model)

   Menerapkan algoritma XGBoost untuk membangun model deteksi multi-klasifikasi. Melakukan pengaturan seleksi fitur dan hyperparameter (tuning) untuk mengoptimalkan performa model.

5. Tahap Kelima (Pengujian dan Evaluasi)

   Tahap selanjutnya adalah kelanjutan dari pengembangan model yang telah diselesaikan. Pada tahap ini, serangan siber diidentifikasi menggunakan sistem deteksi. Kemudian, mengukur performa model dan membandingkan hasil model XGBoost dengan algoritma lainnya.

6. Tahap Keenam (Analisa)

   Menganalisis kelebihan dan kekurangan model XGBoost berdasarkan hasil eksperimen. Membahas dampak preprocessing data dan hyperparameter tuning terhadap kinerja deteksi serangan.

7. Tahap Ketujuh (Kesimpulan dan Saran)

   Membuat kesimpulan berdasarkan penelitian dan menyarankan cara melakukan penelitian lebih lanjut, terutama yang berkaitan dengan sistem IDS dan serangan siber.

1.7 Sistematika Penulisan

Untuk membuat laporan tugas akhir ini lebih mudah dipahami, penulis menggunakan metode penulisan sistematis dalam prosesnya. Adapun sistematika penulisan pada tugas akhir ini sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah yang mendasari penelitian, rumusan masalah, tujuan penelitian, keuntungan dan kekurangan penelitian, serta metodologi penelitian yang singkat, dan prosedur penulisan skripsi.

BAB II TINJAUAN PUSTAKA

Bab ini berisi mengenai dasar teori yang berkaitan dengan konsep dasar IDS, penjelasan tentang serangan siber dan jenis-jenisnya, algoritma XGBoost, dan teori lainnya yang berkaitan dengan subjek penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini memberikan penjelasan menyeluruh tentang proses penelitian. Tujuan dari penjelasan yang ada di bab ini adalah untuk memberikan pembaca gambaran yang jelas dan sistematis tentang cara penelitian dilakukan, sehingga mereka dapat memahami proses dan mengakui validitas temuan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan temuan penelitian dan menganalisisnya untuk menjawab pertanyaan dan mencapai tujuan. Tujuan dari bab ini adalah untuk memberikan pemahaman yang mendalam tentang relevansi, kekuatan, dan kelemahan temuan penelitian, serta bagaimana hal itu berdampak pada pengembangan sistem keamanan jaringan berbasis pengenalan intrusi (IDS).

BAB V KESIMPULAN DAN SARAN

Bab ini memuat kesimpulan dari hasil penelitian yang telah dilakukan, jawaban atas tujuan yang ingin dicapai, serta saran untuk penelitian di masa mendatang.

DAFTAR PUSTAKA

[1] K. Neupane, R. Haddad, and L. Chen, "Next Generation Firewall for Network Security: A Survey," *Conference Proceedings - IEEE SOUTHEASTCON*, vol. 2018-April, pp. 1–6, 2018, doi: 10.1109/SECON.2018.8478973.

[2] Cisco, "Cisco Annual Internet Report (2018–2023) White Paper," Cisco Systems, Inc., San Jose, CA, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[3] P. Devan and N. Khare, "An efficient XGBoost–DNN-based classification model for network intrusion detection system," *Neural Comput Appl*, vol. 32, no. 16, pp. 12499–12514, 2020, doi: 10.1007/s00521-020-04708-x.

[4] A. Husain, A. Salem, C. Jim, and G. Dimitoglou, "Development of an Efficient Network Intrusion Detection Model Using Extreme Gradient Boosting (XGBoost) on the UNSW-NB15 Dataset," *2019 IEEE 19th International Symposium on Signal Processing and Information Technology, ISSPIT 2019*, no. December 2019, 2019, doi: 10.1109/ISSPIT47144.2019.9001867.

[5] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[6] H. Tyagi and R. Kumar, "Attack and anomaly detection in IoT networks using supervised machine learning approaches," *Revue d'Intelligence Artificielle*, vol. 35, no. 1, pp. 11–21, 2021, doi: 10.18280/ria.350102.

[7] J. L. G. Torres, C. A. Catania, and E. Veas, "Active learning approach to label network traffic datasets," *Journal of Information Security and Applications*, vol. 49, p. 102388, Dec. 2019, doi: 10.1016/j.jisa.2019.102388.

[8] M. Mimura, "Adjusting lexical features of actual proxy logs for intrusion detection," *Journal of Information Security and Applications*, vol. 50, p. 102408, Feb. 2020, doi: 10.1016/j.jisa.2019.102408.

[9] P. Kumar, G. P. Gupta, and R. Tripathi, “An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks,” *Comput Commun*, vol. 166, pp. 110–124, Jan. 2021, doi: 10.1016/j.comcom.2020.12.003.

[10] T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, vol. 13-17-Augu, pp. 785–794, 2016, doi: 10.1145/2939672.2939785.

[11] A. E. Onyebueke, A. David, and S. Munu, “Network Intrusion Detection System Using XGBoost and Random Forest Algorithms,” *Asian Journal of Pure and Applied Mathematics*, vol. 5, no. 1, pp. 321–335, 2023, [Online]. Available: https://hal.science/hal-05132990

[12] K. A. Binsaeed and A. M. Hafez, “Enhancing Intrusion Detection Systems with XGBoost Feature Selection and Deep Learning Approaches,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, pp. 1084–1098, 2023, doi: 10.14569/IJACSA.2023.01405112.

[13] S. S. Dhaliwal, A. Al Nahid, and R. Abbas, “Effective intrusion detection system using XGBoost,” *Information (Switzerland)*, vol. 9, no. 7, 2018, doi: 10.3390/info9070149.

[14] A. M. OYELAKIN, “A Learning Approach for The Identification of Network Intrusions Based on Ensemble XGBoost Classifier,” *Indonesian Journal of Data and Science*, vol. 4, no. 3, pp. 190–197, 2024, doi: 10.56705/ijodas.v4i3.88.