Executive Summary

of

the thesis entitled

Anomaly Intrusion Detection and Classification using Machine Learning

Submitted By

Gondalia Archana Bharatbhai (FOTE/997)

Under Guidance of

Dr. Apurva Shah

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
FACULTY OF TECHNOLOGY AND ENGINEERING
THE MAHARAJA SAYAJIRAO UNIVERSITY OF BARODA
VADODARA 390 001

December 2025

TABLE OF CONTENT OF THE EXECUTIVE SUMMARY

Contents

Introduction

Intrusion detection and classification have become fundamental components of modern network security due to the rapid growth of interconnected systems and the increasing sophistication of cyberattacks. Traditional security mechanisms such as firewalls and signature-based detection tools are inadequate for identifying complex and previously unseen threats, leading to a growing reliance on Intrusion Detection Systems (IDS) [**ravi2022**, **bowen2023**]. Among different IDS paradigms, anomaly-based IDS play a crucial role by modeling normal network behavior and detecting deviations that may indicate novel or zero-day attacks [**thakkar2022**]. However, the effectiveness of anomaly-based IDS is strongly influenced by the quality and dimensionality of input features, where high-dimensional and redundant data often result in increased false positive rates and computational overhead [**umar2020**]. Although conventional feature selection methods—filter, wrapper, and embedded techniques—have been widely used, they struggle to handle nonlinear and high-dimensional network traffic efficiently [**li2021**]. To address these challenges, metaheuristic optimization algorithms such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Grey Wolf Optimization (GWO) have been explored for IDS feature selection due to their global search capabilities [**laamari2014**, **zhang2019**]. Despite its advantages, standard GWO employs a static leadership hierarchy, which limits adaptability and may cause premature convergence in dynamic cybersecurity environments [**gondalia2025**]. Motivated by these limitations, this research proposes a Dynamic Grey Wolf Optimization (DGWO)-based framework to enhance feature selection effectiveness, robustness, and interpretability in anomaly-based IDS.

Problem Description and Research Gap

Traditional intrusion detection approaches predominantly rely on signature-based methods that are effective for identifying known attack patterns but fail to detect zero-day or previously unseen threats, necessitating the use of anomaly-based Intrusion Detection Systems (IDS). Although anomaly-based IDS offer the capability to detect novel attacks by modeling deviations from normal network behavior, their practical deployment is hindered by high false positive rates, scalability challenges, and reduced efficiency when processing high-dimensional and heterogeneous network traffic data. Feature selection has been widely adopted to mitigate these issues; however, conventional filter, wrapper, and embedded techniques struggle to handle nonlinear relationships and dynamically evolving cybersecurity datasets. Metaheuristic-based feature selection methods such as Genetic Algorithms, Particle Swarm Optimization, and standard Grey Wolf Optimization have shown promise, yet they remain limited by static search behavior, premature convergence, and

poor adaptability to changing attack patterns. Furthermore, existing IDS research largely prioritizes detection accuracy while overlooking two critical gaps: computational efficiency required for real-time operation and interpretability necessary for analyst trust and practical adoption. Consequently, there is a clear research gap in developing an anomaly-based IDS framework that simultaneously achieves adaptive feature selection, reduced computational overhead, low false positive rates, and model interpretability, while maintaining robustness and generalization across diverse network environments.

Motivation

The motivation for this research arises from the growing dependence on Intrusion Detection Systems (IDS) to safeguard modern networks against increasingly complex and evolving cyber threats. Machine learning and deep learning techniques have shown significant promise in anomaly-based intrusion detection by effectively modeling nonlinear patterns in high-dimensional network traffic data, achieving strong performance on benchmark datasets such as NSL-KDD and UNSW-NB15. However, the presence of redundant and irrelevant features often degrades detection accuracy, increases computational cost, and limits model robustness, making feature selection a critical challenge in IDS design. Although metaheuristic optimization methods such as Genetic Algorithms, Particle Swarm Optimization, and Grey Wolf Optimization have been applied to address this issue, their static search behavior and susceptibility to premature convergence reduce adaptability in dynamic threat environments. Moreover, beyond predictive performance, real-world IDS deployment demands computational efficiency and interpretability to support real-time monitoring and analyst decision-making. Integrating explainable AI techniques, such as Local Interpretable Model-agnostic Explanations (LIME), with optimization-driven feature selection provides an opportunity to enhance both trust and usability. These considerations motivate the development of a dynamic, efficient, and interpretable IDS framework that overcomes the limitations of existing methods while meeting the practical requirements of modern cybersecurity systems.

Problem Statement

Security risks associated with increasingly sophisticated cyberattacks pose a serious challenge to modern networked systems, particularly as attackers continuously adapt their strategies to evade traditional defense mechanisms. Anomaly-based Intrusion Detection Systems (IDS) driven by machine learning and deep learning have shown strong potential for detecting both known and unknown attacks; however, these systems remain vulnerable to high false positive rates, excessive computational overhead, and performance degradation caused by redundant and high-dimensional network features. Existing feature selection methods and static metaheuristic algorithms often fail to adapt to dynamic traffic patterns

and evolving attack behaviors, leading to premature convergence and suboptimal detection performance. Moreover, the lack of interpretability in many high-performing IDS models limits their practical adoption, as security analysts require transparent and explainable decision-making to trust and act upon system alerts. Therefore, there is an urgent need to develop an adaptive, computationally efficient, and interpretable IDS framework that can robustly select meaningful features, generalize across diverse attack scenarios, and provide reliable intrusion detection in real-world, dynamic cybersecurity environments.

Objectives

The primary objectives of this research are highlighted below:

- To design a Dynamic Grey Wolf Optimization (DGWO) algorithm that adapts leadership based on recent fitness trends, thereby enhancing the balance between exploration and exploitation.
- To apply DGWO for feature selection in Intrusion Detection Systems and evaluate its effectiveness across both binary and multiclass classification tasks using benchmark datasets.
- To compare DGWO-selected feature subsets with standard GWO and full-feature baselines using diverse machine learning and deep learning classifiers.
- To incorporate explainable AI (XAI) methods such as Local Interpretable Model-agnostic Explanations (LIME) to interpret the selected features and validate their relevance for security analysis.
- To propose a new Efficiency Index that jointly considers accuracy, F1-score, and execution time, thereby providing a holistic performance assessment of IDS models.

Scope

The primary scope of this research is the development of an anomaly-based intrusion detection framework that integrates Dynamic Grey Wolf Optimization–based feature selection with machine learning and deep learning classifiers for robust cyberattack detection and classification. The study focuses on benchmark network intrusion datasets, namely NSL-KDD and UNSW-NB15, to evaluate the effectiveness of the proposed approach across both binary and multiclass intrusion detection scenarios. To address the challenges of high-dimensional and heterogeneous network traffic data, the research investigates optimization-driven feature selection for reducing redundancy while preserving attack-relevant information. Multiple classifiers, including Random Forest, Support Vector Machine, XGBoost, and Deep Neural Networks, are employed to assess detection performance, computational

efficiency, and generalization capability. Furthermore, the scope includes the integration of explainable AI techniques, specifically Local Interpretable Model-agnostic Explanations (LIME), to validate the interpretability and semantic relevance of selected features. The evaluation is carried out using comprehensive performance metrics such as accuracy, F1-score, false positive rate, execution time, and the proposed Efficiency Index (EF), ensuring the practical relevance and applicability of the framework to real-world intrusion detection environments.

Research Methodology for Work Done

The research primarily focuses on the development of a Dynamic Grey Wolf Optimization–based Feature Selection (DGWO-FS) framework designed to enhance the performance of anomaly-based Intrusion Detection Systems. The proposed methodology integrates an adaptive leadership strategy within the standard Grey Wolf Optimization algorithm to overcome static search behavior and premature convergence, enabling effective selection of discriminative and semantically relevant network features. The selected feature subsets are evaluated using multiple machine learning and deep learning classifiers, including Random Forest, Support Vector Machine, XGBoost, and Deep Neural Networks, to assess detection accuracy, robustness, and generalization across diverse attack scenarios. To ensure interpretability and practical applicability, the framework incorporates explainable AI techniques, specifically Local Interpretable Model-agnostic Explanations (LIME), which provide instance-level explanations and validate the relevance of selected features in intrusion detection decisions.

To support the primary contribution, comprehensive data preprocessing and feature engineering strategies are employed to handle the heterogeneity and high dimensionality of network traffic data. These include data normalization, categorical feature encoding, class imbalance handling, and noise reduction to improve data consistency and learning efficiency. The proposed DGWO-FS framework is evaluated on benchmark datasets such as NSL-KDD and UNSW-NB15 under both binary and multiclass classification settings. Performance is measured using accuracy, F1-score, false positive rate, execution time, and the proposed Efficiency Index (EF), demonstrating that the methodology achieves improved detection performance, reduced computational cost, and enhanced interpretability compared to baseline feature selection and classification approaches.

Conclusion

The conclusion of this research work is presented in this section, summarizing the key findings and contributions achieved through the proposed methodology. The subsequent section outlines potential directions for future research.

Intrusion detection remains a critical component of modern cybersecurity infrastructures due to the continuously evolving nature of cyber threats and the limitations of traditional security mechanisms. This research proposed a novel and adaptive anomaly-based intrusion detection framework that integrates Dynamic Grey Wolf Optimization–based Feature Selection (DGWO-FS) with machine learning and deep learning classifiers to enhance detection accuracy, computational efficiency, and interpretability. By addressing the static leadership limitation of conventional Grey Wolf Optimization, the proposed DGWO-FS framework demonstrated improved adaptability, reduced premature convergence, and more effective exploration of the feature search space across diverse network traffic patterns.

Extensive experimental evaluation on benchmark datasets, including NSL-KDD and UNSW-NB15, under both binary and multiclass classification scenarios, confirmed the effectiveness of the proposed approach. The results showed consistent improvements in accuracy and F1-score, significant reductions in false positive rates, and noticeable gains in execution time when compared with full-feature models and baseline metaheuristic approaches. To provide a holistic assessment of performance that balances predictive effectiveness and computational cost, a novel Efficiency Index (EF) was formulated and validated, demonstrating the superiority of DGWO-FS in achieving an optimal trade-off between detection quality and runtime efficiency.

Furthermore, the integration of explainable AI through Local Interpretable Model-agnostic Explanations (LIME) validated that the features selected by DGWO-FS are not only statistically significant but also semantically meaningful and aligned with human-understandable attack behaviors. This interpretability enhances trust, transparency, and practical applicability of the proposed IDS framework, addressing a major limitation of many existing machine learning and deep learning–based intrusion detection solutions.

The problem statement of this research was defined as follows:

“To develop an adaptive, computationally efficient, and interpretable anomaly-based intrusion detection framework that can effectively reduce feature dimensionality, minimize false positives, and generalize across diverse and evolving cyberattack scenarios.”

A comprehensive literature survey was conducted to identify existing limitations in feature selection and IDS design, leading to the development of the DGWO-FS framework combined with multiple classifiers and explainability mechanisms. All the objectives outlined in this research were successfully achieved, including adaptive feature se-

lection, improved detection performance, reduced computational overhead, and enhanced interpretability. Overall, the proposed DGWO-FS–based IDS framework offers a scalable, robust, and practical solution for modern network security environments and provides a strong foundation for future research in optimization-driven and explainable intrusion detection systems.

Outcome of Research Work

The primary aim of this research was to design and develop an adaptive, computationally efficient, and interpretable anomaly-based Intrusion Detection System (IDS) capable of accurately detecting and classifying cyberattacks in high-dimensional and dynamic network traffic environments. The proposed framework emphasizes optimization-driven feature selection, robustness across diverse datasets, and practical deployability through reduced false alarms and execution time. This section presents a detailed description of the research objectives and their corresponding achievements.

Objective 1: To investigate and analyze existing anomaly-based IDS techniques, feature selection strategies, and metaheuristic optimization algorithms used for network intrusion detection.

Achievement 1: To accomplish this objective, an extensive literature survey was conducted covering traditional and learning-based IDS approaches, with a particular focus on feature selection techniques and metaheuristic algorithms such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and standard Grey Wolf Optimization (GWO). The analysis highlighted critical limitations in existing methods, including static search behavior, premature convergence, high false positive rates, and lack of interpretability. This study provided a clear understanding of current research gaps and motivated the development of a dynamic and adaptive feature selection framework for IDS.

Objective 2: To propose a novel Dynamic Grey Wolf Optimization–based Feature Selection (DGWO-FS) framework that overcomes the limitations of static metaheuristic algorithms.

Achievement 2: To fulfill this objective, a Dynamic Grey Wolf Optimization (DGWO) algorithm was developed by introducing an adaptive leadership mechanism that dynamically updates the alpha, beta, and delta wolves across iterations. This approach improved exploration–exploitation balance and reduced premature convergence during feature selection. The DGWO-FS framework effectively reduced feature dimensionality while preserving semantically relevant and attack-discriminative features, resulting in improved detection performance and computational efficiency compared to standard GWO and full-feature baselines.

Objective 3: To integrate multiple machine learning and deep learning classifiers with DGWO-FS for robust intrusion detection and classification.

Achievement 3: The proposed DGWO-FS framework was integrated with multiple classifiers, including Random Forest, Support Vector Machine, XGBoost, and Deep Neural Networks. Extensive experiments were conducted under both binary and multiclass classification settings to evaluate robustness and generalization capability. The results demonstrated consistent improvements in accuracy, F1-score, and reduced false positive rates across classifiers, confirming the effectiveness of DGWO-FS in enhancing IDS performance under diverse attack scenarios.

Objective 4: To validate the proposed framework on benchmark intrusion detection datasets and evaluate its computational efficiency.

Achievement 4: The proposed methodology was empirically validated using widely adopted benchmark datasets, namely NSL-KDD and UNSW-NB15. Comprehensive preprocessing, normalization, and feature engineering steps were applied to ensure data consistency. Performance evaluation using metrics such as accuracy, F1-score, false positive rate, execution time, and convergence behavior confirmed that DGWO-FS outperformed baseline feature selection approaches while significantly reducing computational overhead, making it suitable for real-time IDS deployment.

Objective 5: To enhance the interpretability and trustworthiness of the IDS using explainable AI techniques.

Achievement 5: To address interpretability, the framework incorporated Local Interpretable Model-agnostic Explanations (LIME) to analyze and validate the contribution of selected features at the instance level. LIME-based explanations demonstrated that the features selected by DGWO-FS are not only statistically significant but also semantically meaningful and aligned with human-understandable attack behaviors. This enhanced transparency and trust in the IDS decision-making process.

Objective 6: To propose a unified performance evaluation metric that jointly considers detection effectiveness and computational efficiency.

Achievement 6: A novel Efficiency Index (EF) was formulated by combining accuracy, F1-score, and execution time into a single metric. The EF index provided a balanced assessment of IDS performance and clearly demonstrated the superiority of DGWO-FS over full-feature and baseline approaches across datasets and classifiers. This index offers a practical tool for evaluating IDS suitability in resource-constrained and real-time environments.

In summary, all the objectives outlined in this research were successfully achieved. The proposed DGWO-FS–based IDS framework delivers improved detection accuracy, reduced false positive rates, enhanced computational efficiency, and meaningful interpretability, thereby providing a scalable and robust solution for modern intrusion detection systems.

Key Findings

- Effectiveness of Optimization-Driven Feature Selection: This study demonstrates that optimization-based feature selection significantly improves anomaly-based IDS performance by reducing feature dimensionality while preserving attack-discriminative information. Dynamic Grey Wolf Optimization (DGWO) outperforms traditional feature selection methods and static metaheuristics by adapting to evolving network traffic patterns.
- Improved Detection Accuracy and Reduced False Positives: The proposed DGWO-FS framework consistently achieves higher accuracy and F1-score, along with substantial reductions in false positive rates across both binary and multiclass intrusion detection tasks on NSL-KDD and UNSW-NB15 datasets.
- Enhanced Computational Efficiency for Real-Time IDS: By selecting a compact and informative feature subset, DGWO-FS significantly reduces execution time and improves convergence speed across multiple classifiers, making the framework suitable for real-time and resource-constrained intrusion detection environments.
- Generalization Across Classifiers and Datasets: Experimental results confirm that DGWO-FS exhibits robust generalization when integrated with diverse classifiers, including Random Forest, SVM, XGBoost, and Deep Neural Networks, and maintains consistent performance across heterogeneous datasets and attack types.
- Interpretability Through Explainable AI: The integration of Local Interpretable Model-agnostic Explanations (LIME) validates that the features selected by DGWO-FS are semantically meaningful and aligned with human-understandable attack behaviors, enhancing trust and transparency in IDS decision-making.
- Balanced Performance Evaluation Using Efficiency Index (EF): The proposed Efficiency Index (EF), which jointly considers detection effectiveness and computational cost, provides a comprehensive performance assessment and highlights the practical superiority of DGWO-FS over full-feature and baseline approaches.

Future Work

The proposed Dynamic Grey Wolf Optimization–based Feature Selection (DGWO-FS) framework establishes a strong foundation for efficient, adaptive, and interpretable anomaly-based intrusion detection. However, several promising directions remain open for future research. Extending the evaluation to larger, more diverse, and real-time network

traffic datasets, including emerging IoT and cloud-based environments, will further validate the scalability and generalizability of the proposed approach. Future work may also explore the integration of DGWO-FS within end-to-end security monitoring systems, such as Software-Defined Networking (SDN) and edge-based intrusion detection architectures, to assess real-time detection capability and operational reliability.

Additionally, incorporating online or incremental learning mechanisms can enable the IDS to dynamically adapt to evolving attack patterns without requiring complete retraining. Hybridizing DGWO with other adaptive or self-learning optimization strategies may further enhance exploration–exploitation balance under highly dynamic threat landscapes. Expanding explainability through advanced XAI techniques beyond LIME, such as SHAP or counterfactual explanations, could provide deeper insights into IDS decision-making and strengthen analyst trust. Finally, developing lightweight and energy-efficient variants of the DGWO-FS framework for deployment in resource-constrained environments, such as IoT and edge computing platforms, represents a valuable direction for advancing practical and scalable intrusion detection solutions.

Bibliography

AIT TCHAKOUCHT, T., & EZZIYYANI, M. (2018). Building a fast intrusion detection system for high-speed-networks: Probe and dos attacks detection. *Procedia Computer Science*, *127*, 521-530. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050918301637 (Proceedings of The First International Conference on Intelligent Computing In Data Sciences, ICDS2017) doi: https://doi.org/10.1016/j.procs.2018.01.151

Ali, A., Assam, M., Khan, F. U., Ghadi, Y. Y., Nurdaulet, Z., Zhibek, A., ... Alahmadi, T. J. (2024). An optimized multilayer perceptron-based network intrusion detection using gray wolf optimization. *Computers and Electrical Engineering*, *120*, 109838. Retrieved from https://www.sciencedirect.com/science/article/pii/S0045790624007651 doi: https://doi.org/10.1016/j.compeleceng.2024.109838

Almomani, O. (2020). A feature selection model for network intrusion detection system based on pso, gwo, ffa and ga algorithms. *Symmetry*, *12*(6). Retrieved from https://www.mdpi.com/2073-8994/12/6/1046 doi: 10.3390/sym12061046

Arafah, M., Phillips, I., Adnane, A., Hadi, W., Alauthman, M., & Al-Banna, A.-K. (2025). Anomaly-based network intrusion detection using denoising autoencoder and wasserstein gan synthetic attacks. *Applied Soft Computing*, *168*, 112455. Retrieved from https://www.sciencedirect.com/science/article/pii/S1568494624012298 doi: https://doi.org/10.1016/j.asoc.2024.112455

Azizjon, M., Jumabek, A., & Kim, W. (2020). 1d cnn based network intrusion detection with normalization on imbalanced data. In *2020 international conference on artificial intelligence in information and communication (icaiic)* (p. 218-224). doi: 10.1109/ICAIIC48513.2020.9064976

B, S., & K, M. (2019). Firefly algorithm based feature selection for network intrusion detection. *Computers Security*, *81*, 148-155. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404818303936 doi: https://doi.org/10.1016/j.cose.2018.11.005

Bowen, B., Chennamaneni, A., Goulart, A., & Lin, D. (2023a). Blocnet: a hybrid, dataset-independent intrusion detection system using deep learning. *International Journal of Information Security*, *22*(4), 893-917. Retrieved from https://research.ebsco.com/linkprocessor/plink?id=4f07e34f-3e40-3956-b0c3-50f7af9cf066

Bowen, B., Chennamaneni, A., Goulart, A., & Lin, D. (2023b, August). BLoCNet: a hybrid, dataset-independent intrusion detection system using deep learning. *Int. J. Inf. Secur.*, *22*(4), 893–917.

Breiman, L. (2001). Random forests. *Machine Learning*, *45*(1), 5–32.

Chen, T., & Guestrin, C. (2016). Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd* (pp. 785–794).

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning*, *20*(3), 273–297.

Cui, J., Zong, L., Xie, J., & Tang, M. (2023). A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. *Appl. Intell.*, *53*(1), 272–288.

Dey, P., & Bhakta, D. (2023). A new random forest and support vector machine-based intrusion detection model in networks. *National Academy Science Letters*, *46*(5), 471–477. Retrieved from `https://doi.org/10.1007/s40009-023-01223-0` doi: 10.1007/s40009-023-01223-0

Drewek-Ossowicka, A., Pietrołaj, M., & Rumiński, J. (2021). A survey of neural networks usage for intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 497–514. Retrieved from `https://doi.org/10.1007/s12652-020-02014-x` doi: 10.1007/s12652-020-02014-x

Eesa, A., Orman, Z., & Abdulazeez, A. (2015, 01). A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems.

Elmasry, W., Akbulut, A., & Zaim, A. (2019, 06). Empirical study on multiclass classification-based network intrusion detection. *Computational Intelligence*, *35*. doi: 10.1111/coin.12220

Emi. (2025). Explainable ai with lime library. *Medium*. Retrieved from https://medium.com/@emykes/explainable-ai-with-lime-library-4ed5fc0969f4 (Accessed: June 23, 2025)

Eshak Magdy, M., M. MATTER, A., HUSSIN, S., HASSAN, D., & Elsaid, S. (2023). A comparative study of intrusion detection systems applied to nsl-kdd dataset. *The Egyptian International Journal of Engineering Sciences and Technology*, *43*(2), 88-98. Retrieved from https://eijest.journals.ekb.eg/article_258706.html doi: 10.21608/eijest.2022.137441.1156

Golrang, A., Golrang, A. M., Yildirim Yayilgan, S., & Elezaj, O. (2020). A novel hybrid ids based on modified nsgaii-ann and random forest. *Electronics*, *9*(4). Retrieved from https://www.mdpi.com/2079-9292/9/4/577 doi: 10.3390/electronics9040577

Gondalia, A., & Shah, A. (2025, March). Enhancing intrusion detection system reliability using gwo-somnn (grey wolf optimization with self-organizing map neural network). *Reliability: Theory & Applications*, *1*(82), 883–896. Retrieved from https://www.gnedenko.net/Journal/2025/012025/RTA_1_2025-70.pdf doi: 10.24412/1932-2321-2025-182-883-896

Gupta, M., & Shrivastava, S. (2015, 02). Intrusion detection system based on svm and bee colony. *International Journal of Computer Applications*, *111*, 27-32. doi: 10.5120/19576-1377

Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Cnn-lstm: Hybrid deep neural network for network in-

trusion detection system. *IEEE Access*, *10*, 99837-99849. doi: 10.1109/ACCESS.2022.3206425

Imamverdiyev, Y., & Abdullayeva, F. (2018). Deep learning method for denial of service attack detection based on restricted boltzmann machine. *Big Data*, *6*(2), 159-169. Retrieved from https://doi-org.ahdunielib.remotexs.in/10.1089/big.2018.0023 (PMID: 29924649) doi: 10.1089/big.2018.0023

Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access*, *8*, 32464-32476. doi: 10.1109/ACCESS.2020.2973730

Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a recurrent neural networks based framework. *Computer Communications*, *199*, 113-125. Retrieved from https://www.sciencedirect.com/science/article/pii/S0140366422004601 doi: https://doi.org/10.1016/j.comcom.2022.12.010

Kasongo, S. M., & Sun, Y. (2020). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers Security*, *92*, 101752. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404820300365 doi: https://doi.org/10.1016/j.cose.2020.101752

Kohonen, T. (2006). Self-organizing neural projections. *Neural Networks*, *19*(6), 723-733. Retrieved from https://www.sciencedirect.com/science/article/pii/S0893608006000645 (Advances in Self Organising Maps - WSOM'05) doi: https://doi.org/10.1016/j.neunet.2006.05.001

Laamari, M. A., & Kamel, N. (2014, 01). A hybrid bat based feature selection approach for intrusion detection. In (Vol. 472, p. 230-238). doi: 10.1007/978-3-662-45049-9_38

Li, L.-H., Ahmad, R., Tsai, W.-C., & Sharma, A. K. (2021). A feature selection based dnn for intrusion detection system. In *2021 15th international conference on ubiquitous information management and communication (imcom)* (p. 1-8). doi: 10.1109/IMCOM51814.2021.9377405

Liu, Z., & Shi, Y. (2022). A hybrid ids using ga-based feature selection method and random forest. *International Journal of Machine Learning and Computing*. Retrieved from `https://api.semanticscholar.org/CorpusID:247829090`

Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access*, *8*, 77396-77404. doi: 10.1109/ACCESS.2020.2986013

Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey wolf optimizer. *Advances in Engineering Software*, *69*, 46-61. Retrieved from `https://www.sciencedirect.com/science/article/pii/S0965997813001853` doi: https://doi.org/10.1016/j.advengsoft.2013.12.007

Mohammed Zakariah, A. M. A. A. A. A., Salman A. AlQahtani. (2023). Intrusion detection system with customized machine learning techniques for nsl-kdd dataset. *Computers, Materials & Continua*, *77*(3), 4025–4054. Retrieved

from http://www.techscience.com/cmc/v77n3/55048 doi: 10.32604/cmc.2023.043752

Mohiuddin, G., Lin, Z., Zheng, J., Wu, J., Li, W., Fang, Y., ... Zeng, X. (2023). Intrusion detection using hybridized meta-heuristic techniques with weighted xgboost classifier. *Expert Systems with Applications*, *232*, 120596. Retrieved from https://www.sciencedirect.com/science/article/pii/S0957417423010989 doi: https://doi.org/10.1016/j.eswa.2023.120596

Moustafa, N. (2015). *The unsw-nb15 dataset.* https://research.unsw.edu.au/projects/unsw-nb15-dataset. (Accessed: November 5, 2025)

Mulyanto, M., Leu, J.-S., Faisal, M., & Yunanto, W. (2023). Weight embedding autoencoder as feature representation learning in an intrusion detection systems. *Computers and Electrical Engineering*, *111*, 108949. Retrieved from https://www.sciencedirect.com/science/article/pii/S0045790623003737 doi: https://doi.org/10.1016/j.compeleceng.2023.108949

Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. *IEEE Access*, *6*, 48231-48246. doi: 10.1109/ACCESS.2018.2863036

of New Brunswick, U. (2009). *Nsl-kdd dataset.* https://www.unb.ca/cic/datasets/nsl.html. (Accessed: November 5, 2025)

Ravi, V., Chaganti, R., & Alazab, M. (2022). Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. *Computers & Electrical Engineering*, *102*, 108156.

Sadaf, K., & Sultana, J. (2020). Intrusion detection based on autoencoder and isolation forest in fog computing. *IEEE Access*, *8*, 167059-167068. doi: 10 .1109/ACCESS.2020.3022855

Singh, R., Kumar, H., & Singla, R. (2015). An intrusion detection system using network traffic profiling and online sequential extreme learning machine. *Expert Systems with Applications*, *42*(22), 8609-8624. Retrieved from https://www.sciencedirect.com/science/article/pii/S0957417415004753 doi: https://doi.org/10.1016/j.eswa.2015.07.015

Thakkar, A., & Lohiya, R. (2020). A review of the advancement in intrusion detection datasets. *Procedia Computer Science*, *167*, 636-645. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050920307961 (International Conference on Computational Intelligence and Data Science) doi: https://doi.org/10.1016/j.procs.2020.03.330

Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*, *55*(1), 453–563. Retrieved from https://doi.org/10.1007/s10462-021-10037-9 doi: 10 .1007/s10462-021-10037-9

Umar, M. A., Chen, Z., Shuaib, K., & Liu, Y. (2025). Effects of feature selection and normalization on network intrusion detection. *Data Science and Management*, *8*(1), 23-39. Retrieved from https://www.sciencedirect.com/science/article/pii/S2666764924000390 doi: https://doi.org/10.1016/j.dsm.2024.08.001

Umar, M. A., Zhanfang, C., & Liu, Y. (2020). Network intrusion detection using wrapper-based decision tree for feature selection. In *Proceedings of the 2020 international conference on internet computing for science and engineering* (p. 5–13). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3424311.3424330 doi: 10.1145/3424311.3424330

Zhang, J., Ling, Y., Chung, Y., Yang, X., Xiong, G., Zhang, R., ... Zhang, C. (2019, 11). Model of the intrusion detection system based on the integration of spatial-temporal features. *Computers Security*, *89*. doi: 10.1016/j.cose.2019.101681

Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020, 06). Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Computer Networks*, *174*. doi: 10.1016/j.comnet.2020.107247