




Review Article

Feature Selection Techniques in Intrusion Detection: A Comprehensive Review

^{1*} Maher Khalaf Hussein 

Computer Center, Presidency
of the University
University of Telafer
Mosul, Iraq.
maher.k.hussein@uotelafer.edu.iq

² Lubna Thanoon ALkahla 

Software Department, Information
Technology College
Ninevah University
Mosul, Iraq.
lubna.thanoon@uoninevah.edu.iq

³ Asmaa Alqassab 

Department of Computer Science, College
of Education for Pure Science
University of Mosul
Mosul, Iraq.
asmaa_mow@uomosul.edu.iq

ARTICLE INFO

Article History

Received:06/01/2024

Accepted :02/02/2024

Published:01/06/2024

This is an open-access
article under the CC
BY 4.0 license:

<http://creativecommons.org/licenses/by/4.0/>

ABSTRACT

Abstract - This investigation aims to explore previous research on the implementation of feature selection in intrusion detection. Feature selection has demonstrated its ability to enhance or sustain comparable classification accuracy levels for intrusion detection systems, while simultaneously improving classification efficiency. The evaluation includes an assessment of filter-based, wrapper-based, and hybrid feature selection techniques. Given that Big Data challenges can affect intrusion detection, feature selection's classification efficiency can aid in lowering computing requirements. Older KDD intrusion detection datasets have received considerable attention in previous feature selection research. Consequently, researchers need more high-quality datasets that are available to the general public.

Keywords: Security, Feature selection, Intrusion detection, Feature Reduction, Cybersecurity.



1. INTRODUCTION

A network intrusion detection system (NIDS) is a security tool that scans network traffic for indications of malicious activity, unauthorized access, and other security risks. The operations of this product mainly include real-time network traffic analysis and comparing it with a known database of attack signatures or patterns, upon which security personnel is then notified by the NIDS for investigation and necessary steps to ensure that the threat is reduced. There are several different ways of utilizing NIDS, one can be on site or cloud-based or managed service. Furthermore, in achieving a fully integrated security posture [1][2], it can be combined with other security technologies. NIDS' demand has increased because of the emergence of new technologies such as cloud computing and the Internet of Things, which have led to an increase in cybercrimes. Therefore, NIDS is remarkably in protecting network infrastructure and preserving data integrity regardless of the size of a company [3].

In detecting and averting cyber-attacks, intrusion detection systems (IDS) are very critical. However, considerable previous research related to this area has some drawbacks. One key problem is that there are very many false positives and negatives causing them to produce unnecessary alarms or miss intrusions, which might paralyze their efficiency. Nevertheless, few IDSs detect some attacks, leaving others undetected and vulnerable. In addition, the high rate of false alarms leads to alert fatigue and reduced efficacy. Moreover, some IDS cannot handle large-scale networks or traffic with high speed or even cope with new forms of attack or changes within a network environment. Finally, some IDS may lack the ability to be integrated with other security tools; hence, they become less effective as part of a comprehensive security

strategy. These limitations and drawbacks call for further research and development on IDS that enhance their accuracy, coverage, scalability, adaptability, and integration capabilities with other security tools [4].

2. INTRUSION DETECTION SYSTEM

NIDSs are network-based IDSs that identify malicious network traffic. NIDS typically necessitate unrestricted network access to examine all network traffic, including unicast traffic. NIDS are passive devices that observe and do not intervene in the traffic they track; an example of a NIDS architecture is illustrated in Figure 1. In read-only mode, the NIDS intercepts the firewall's internal interface and transmits notifications to an NIDS management server through an alternative network interface, which supports writing [5].

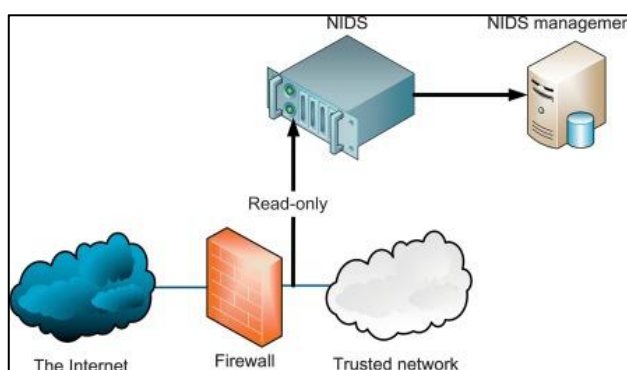


Fig. 1 Structure of an intrusion detection system [6]

3. FEATURE SELECTION TECHNIQUES

Selecting the most essential features from a dataset to be used in training models is called feature selection. This method aims to improve model accuracy by removing redundant data, reducing input variables, and simplifying complex models. With feature selection, the risk of overfitting is minimized, training time is shortened, and the accuracy of the model is increased [7].

Using feature selection techniques that identify important aspects within network traffic data combined with NIDS can produce a victorious network security strategy. Improved NIDS accuracy in identifying and responding to security threats results from such amalgamation. This, in turn, can potentially ameliorate the system's performance by minimizing false positives. [8]

Selection of features can be performed in various ways, some of which are as follows:

1. Feature selection can be achieved through filter methods that assess the importance of each feature. These methods employ statistical measures such as correlation or mutual information. The top-ranking features are picked without consideration for their interactions with one another. Some illustrations include feature selection based on correlation or mutual information [9][10].
2. Wrapper methods: These techniques evaluate the performance of a machine learning (ML) model using different subsets of features. It trains the model on each subset and then measures its performance on a validation set. From this, the best subset is obtained with regard to performance, for example, forward selection and backward elimination [11] [12].
3. Embedded methods: These techniques integrate feature selection into the model training process. During training, the model will choose those features that are most relevant to it, for example, Lasso regression and decision trees (DT) [13] [14].



4. Hybrid methods: These techniques combine multiple feature selection techniques to enhance their effectiveness, for example, if a hybrid method takes advantage of a filter technique to prune a potential feature list before using a wrapper method for selection [15] [16].

The choice of feature selection technique depends on factors such as dataset size, number of features, model complexity, and target variable; thus, careful evaluation and comparison among various feature selection techniques should be made to determine which one is most suitable for a particular problem.

4. DATASET

Publicly available datasets for NIDs are widely used for research and development purposes, some of which are as follows:

1. KDD Cup 1999 Dataset: It is a big collection of network traffic records that have been labeled as normal or attack. The types of attacks in it include DoS, Probe, U2R, and R2L [17] [18].
2. NSL-KDD Dataset: It is an improvement of the KDD Cup 1999 dataset, which covers issues such as redundancy and imbalanced data distribution. Some examples of attacks featured here are DoS, Probe, U2R, and R2L [19].
3. UNSW-NB15 Dataset: This comprehensive dataset contains normal and attack traffic that is derived from a real network environment. A total of nine categories encompasses this system: Denial of Service (DoS), Probe, User to Root (U2R), Remote to Local (R2L), and shellcode [20] [21].
4. The CIC-IDS2017 dataset ranks among the important resources as far as cybersecurity is concerned. The Canadian Institute for Cybersecurity was the source of the dataset that was used in this research. It avails network traffic data containing normal and attack patterns. Various categories of attacks such as DoS, Network Probing, and Web-based Attacks are discussed in this paper [22].
5. The CSE-CICIDS2018 dataset stands for the Canadian Institute for Cybersecurity–Cybersecurity Intrusion Detection Standard Dataset 2018. It is a publicly accessible dataset established for testing and validating IDSs. The University of New Brunswick’s Canadian Institute for Cybersecurity has developed a comprehensive framework with a wide range of attack techniques [23] [24].
6. The CTU-13 Dataset contains network traffic data that were collected over several months by Czech Technical University. The system includes different types of cyber-attacks such as DoS, Botnet, and Port Scanning [25].
7. These datasets not only play a role in training and evaluating ML models for network intrusion detection but also enable comparisons between various algorithm and feature selection techniques. All datasets can be downloaded from the Kaggle website: <https://www.kaggle.com/datasets>.

5. RELATED WORKS

The reviewed studies delve into various methodologies for improving IDSs. In [26], the XGBoost algorithm is explored for feature selection, in conjunction with ANN, SVM, LR, DT, and Knn classifiers, using the UNSW-NB15 dataset for evaluation in binary and multiclass settings. The XGBoost-based attribute selection yields 19 optimal features, and a literature review compares various classifiers’ performance. Notably, a reduced feature vector enhances detection accuracy and reduces model complexity, resulting in improved binary classification accuracy for DT.

In [27], a novel feature selection algorithm based on pigeon-inspired optimizers (PIO) is proposed for IDSs, achieving robustness, high detection rates, accuracy, and low false alarms. Compared with traditional methods, the PIO algorithm exhibits faster convergence, utilizing cosine similarity-based discretization. Furthermore, a wrapper feature selection algorithm outperforms other methods with regard to TPR, FPR, accuracy, and F-score.

In [28] and [29], different ML models are presented with various algorithms and feature selection methods for classifying network traffic and detecting known and novel attacks. The ANN-based model with wrapper feature selection demonstrates superior performance in network traffic classification, contributing to advancements in IDS research. This study uses the NSL-KDD dataset to evaluate model efficiency.

In [30], the HFS-KODE hybrid approach combines CfsSubstEval, genetic search, and a rule-based engine for feature selection, along with an ensemble classifier utilizing K-means, One-Class SVM, DBSCAN, and Expectation-Maximization. The HFS-KODE model outperforms individual classifiers and state-of-the-art feature selection methods,



achieving impressive accuracy on CIC-IDS2017, NSL-KDD, and UNSW-NB15 datasets, while reducing false-alarm rates and model building/testing time.

In [31], MIMCA is proposed as a feature selection technique based on diversification in Multicast Convolutional Algorithm (MCA). MIMCA outperforms standard methods, optimizing the generation of classified rules and improving IDS speed in network security through mutual information utilization.

In [32], an enhanced BPSO approach is introduced for discrete feature selection in NIDS, resulting in increased accuracy, detection rate, and reduced false-alarm reports. The approach incorporates a fully connected dense deep neural network for flow-based intrusion detection on the CSE-CIC-IDS2018 dataset, showcasing a high accuracy of 95% compared with benchmark classifiers.

Moreover, [33] proposes a NIDS that combines Whale optimization algorithm (WOA) and genetic algorithms (GA) for feature selection and KNN-based classification, leading to better results than previous methods. The WOA and GA extract features relevant to class labels, enabling effective detection of misconduct nodes in wireless networks.

In addition, [34] introduces two feature selection and intrusion detection models (PSO-GWO-NB and PSO-GWO-ANN), using PSO and GWO algorithms, and evaluates their performance with reduced feature sets. The intersection of (PSO and GWO) features yields promising results with minimum feature sets, demonstrating their acceptability for intrusion detection.

In [35], the LNNLS-KH algorithm is proposed for feature selection in network intrusion detection, using krill swarm intelligence and nonlinear optimization. It is hard to believe that the algorithm outperforms all other methods with regard to feature reduction and detection accuracy. This algorithm has been further compared [36] with a unique intrusion detection approach that utilizes correlation-based feature selection and classifier subset evaluation techniques resulting in fewer attributes and high precision while classifying attacks. The IBK algorithm performs better than MLP in intrusion detection.

The ensemble-based automatic feature selection method for IDSs with large traffic features was designed in [37], which optimizes feature subsets by using NSOM scores. Through this approach, the method has outperformed recent approaches, and considering automatic feature selection, future research into lightweight classification models will be carried out.

The ID-RDRL method takes cues from RFE (Feature Selection) and utilizes deep reinforcement learning [38]. The objective of this model is to enhance IDS efficiency, improve deep reinforcement learning performance, quicken feature selection, and enable dynamic feature selection, all while building a robust interaction between the classifier and environment. This method has been further developed [39] to detect intrusion in complex network environments, subsequently providing an improved IDS performance that features feature selection and deep reinforcement learning. To enhance its effectiveness and efficiency, future studies will prioritize the enhancement of the relationship between the classifier and its surroundings. In addition, [40] extraneous features within IDS datasets will be addressed by integrating filter-based and wrapper-based methods into feature selection. Finally, the IG+FS+DT algorithm, which is an Information Gain plus Chi-Square forward selection combination, shows better accuracy on NSL-KDD and CIC-IDS2017 datasets, suggesting that simpler but more effective IDSs can be built. Table 1 displays the summary of data used in this study.

Table I Summary of Techniques and Datasets

Reference	Year	Dataset	Technique
26	2020	UNSW-NB15	kNN, LR, ANN,SVM and Decision Tree (DT)
27	2020	NSL-KDD	Pigeon Inspired Optimizer.
28	2020	NSL-KDD	support Vector Machine (SVM) and Artificial Neural Networks (ANN)
29	2020	CSE-CICIDS2018	correlation-based univariate, MI-based univariate, and correlation based forward search algorithms
30	2021	CIC-IDS2017, NSL-KDD, and UNSW-NB15	ensemble classifier that used Class SVM, K-means, DBSCAN, and Expectation-Maximization
31	2021	NSL-KDD and UNSW-NB15	Meerkat Clan Algorithm (MCA)

32	2021	CSE-CIC-IDS2018	Binary Particle Swarm Optimization (BPSO), correlation-based (CFS), and deep learning
33	2021	KDDCUP1999	Whale optimization (WOA) and genetic algorithms (GA)
34	2021	UNSW-NB15	PSO-GWO-NB
35	2021	NSL-KDD, CICIDS2017	Krill-swarm algorithm based on linear nearest neighbor
36	2021	CIC IDS-2017	correlation-based feature selection CFS, NB
37	2022	UNSW-NB15, CIC-IDS2017, and CSE-CIC-IDS2018,	XGBoost, ET method, mutual information, mRMR, and Pearson correlation coefficient
38	2022	CSE-CIC-IDS2018	deep reinforcement learning
39	2022	NSL-KDD	InfoGain, Chi-squared attribute evaluation (CHI) with Ranker, Gain Ratio Feature Evaluation with Ranker, and CFS with Greedy Stepwise
40	2023	NSL-KDD, CIC-IDS2017.	Filter-based and wrapper-based methods

6. ANALYSIS AND DISCUSSION

The results of our study indicate that the NSL-KDD datasets are prevalent in research pertaining to the implementation of feature selection for intrusion detection, Among the 15 research samples analyzed in our study, seven of the datasets belong to the Knowledge Discovery in Databases (NSL-KDD) category (Fig. 2 and Table 1). The current research on feature selection and intrusion detection exhibits a limited scope as it predominantly concentrates on a singular dataset. The utilization of outdated datasets, which are over two decades old, persists in contemporary research, exacerbating the issue at hand. The aforementioned datasets have received remarkable criticism from numerous researchers, implying the potential application of feature selection techniques on more recent datasets.

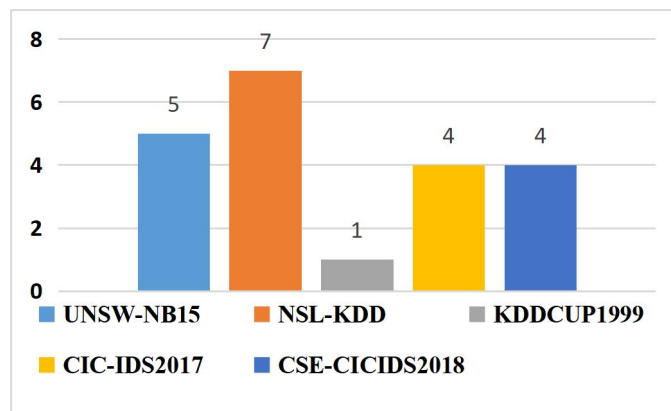


Fig. 2 Number of using the different datasets

Some of the major critiques for obsolete datasets in use in feature selection and intrusion detection research are as follows:

1. **Narrow scope:** The conclusions made from just one set of data may not be completely representative of the range of cyber-attacks that happen daily, thereby limiting their generalizability.
2. **Outdated data:** The current research datasets used are over two decades old, which could make them unable to represent the latest developments in cyber threats and vulnerabilities.
3. **Lack of diversity:** Modern-day research datasets may fail to include a complete range of attack types, thereby making it difficult for them to be used effectively in feature selection analysis.



4. Limitations in scalability: At present, datasets used for research may have some issues when it comes to dealing with large networks or a high-speed traffic; hence, they cannot be used in practice.
5. Limited flexibility: With regard to accommodating

evolving network environments or new attack variations, the currently used datasets in the course of researching can manifest their gradual inefficiency.

Furthermore, several data processing methodologies, including but not limited to data transformation, discretization, data cleaning, and reduction, exhibit restricted applicability, potentially enhancing the effectiveness and precision of the system and detection models.

7. CONCLUSIONS

The proliferation of Internet-connected devices has resulted in a flood of data transferred between them. Data transmission between devices must be encrypted, making network security a key field of study in the modern networking landscape. Thus, IDSs are commonly used alongside other forms of security such as firewalls and access controls. Several different lines of inquiry have been provided to explore the IDS by employing various forms of ML, deep learning, swarm, and evolutionary algorithms.

This survey covers the years 2020 through 2023, and it is representative of the research done in the subject of IDS. The techniques that have included feature selection in their models for performance evaluation are the primary topic of this research. Various IDS datasets are also discussed in the paper.

Acknowledgment

We are deeply grateful to the managing editor and anonymous reviewers for their insightful feedback and comments to enhance the contribution's excellence. Last but not least, we express our heartfelt gratitude to Prof. Manar Younis Kashmola and Dr. Ali Othman suggested that we submit our research work to this prestigious journal.

References

- [1] yang, z., liu, x., li, t., wu, d., wang, j., zhao, y., & han, h. , " a systematic literature review of methods and datasets for anomaly-based network intrusion detection", *computers & security*, 116, 102675,2022.
- [2] Zhang, C., Jia, D., Wang, L., Wang, W., Liu, F., & Yang, A. , "Comparative research on network intrusion detection methods based on machine learning", *Computers & Security*, 102861, 2022.
- [3] He, K., Kim, D. D., & Asghar, M. R. , " Adversarial machine learning for network intrusion detection systems", a comprehensive survey. *IEEE Communications Surveys & Tutorials*,2023.
- [4] Heidari, A., & Jabraeil Jamali, M. A." Internet of Things intrusion detection systems: a comprehensive review and future directions". *Cluster Computing*, 26(6), 3753–3780. <https://doi.org/10.1007/s10586-022-03776-z>, 2022.
- [5] Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. " A systematic literature review for network intrusion detection system (IDS)",*International Journal of Information Security*, 22(5), 1125–1162. <https://doi.org/10.1007/s10207-023-00682-2>,2023.
- [6] Conrad, E., Misener, S., & Feldman, J. , "Eleventh Hour CISSP®. Syngress", Retrieved from http://books.google.ie/books?id=WZo5DAAAQBAJ&pg=PA145&dq=https://doi.org/10.1016/B978-0-12-811248-9.00007-3&hl=&cd=1&source=gbs_api.2016.
- [7] Disha, R. A., & Waheed, S. ",Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique",*Cybersecurity*, 5(1), 1,2022.
- [8] Acharya, N., & Singh, S. , "An IWD-based feature selection method for intrusion detection system", *Soft Computing*, 22, 4407-4416,2018.



- [9] Cherrington, M., Thabtah, F., Lu, J., & Xu, Q. , "Feature selection: filter methods performance challenges", In 2019 International Conference on Computer and Information Sciences (ICCIS), (pp. 1-4). IEEE, April 2019.
- [10] Bommert, A., Welchowski, T., Schmid, M., & Rahnenführer, J. , " Benchmark of filter methods for feature selection in high-dimensional gene expression survival data", *Briefings in Bioinformatics*, 23(1), bbab354,2022.
- [11] Liu, Z., Yang, J., Wang, L., & Chang, Y. " A novel relation aware wrapper method for feature selection", *Pattern Recognition*, 140, 109566. <https://doi.org/10.1016/j.patcog.2023.109566>,2023
- [12] Venkatesh, B., & Anuradha, J. ", A review of feature selection and its methods", *Cybernetics and information technologies*, 19(1), 3-26,2019.
- [13] Liu, H., Zhou, M., & Liu, Q. , "An embedded feature selection method for imbalanced data classification", *IEEE/CAA Journal of Automatica Sinica*, 6(3), 703-715,2019.
- [14] Kothuri, S. R., & N R, D. R. " a hybrid feature selection model for emotion recognition using shuffled frog leaping algorithm (sfla)-incremental wrapper- based subset feature selection" (*iwss*). *indian journal of computer science and engineering*, 13(2), 354–364. <https://doi.org/10.21817/indjcse/2022/v13i2/221302040>,2022.
- [15] Moustafa, N., & Slay, J. , " A hybrid feature selection for network intrusion detection systems", *Central points*. arXiv preprint arXiv,1707.05505,2019.
- [16] Kunhare, N., Tiwari, R., & Dhar, J. " Intrusion detection system using hybrid classifiers with meta-heuristic algorithms for the optimization and feature selection by genetic algorithm", *Computers and Electrical Engineering*, 103, 108383,2022.
- [17] Kumar, S., Gupta, S., & Arora, S. , " A comparative simulation of normalization methods for machine learning-based intrusion detection systems using KDD Cup'99 dataset", *Journal of Intelligent & Fuzzy Systems*, 42(3), 1749-1766,2022.
- [18] Tanimu, J. J., Hamada, M., Robert, P., & Mahendran, A., "Network Intrusion Detection System Using Deep Learning Method with KDD Cup'99 Dataset", In 2022 IEEE 15th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoc) (pp. 251-255). IEEE, December 2022.
- [19] Fuat, T. Ü. R. K. "Analysis of Intrusion Detection Systems in UNSW-NB15 and NSL-KDD Datasets with Machine Learning Algorithms", *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi*, 12(2), 465-477,2023.
- [20] Yin, Y., Jang-Jaccard, J., Xu, W., Singh, A., Zhu, J., Sabrina, F., & Kwak, J. , " IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset", *Journal of Big Data*, 10(1), 1-26,2023.
- [21] Kabir, M. H., Rajib, M. S., Rahman, A. S. M. T., Rahman, M. M., & Dey, S. K. , "Network Intrusion Detection Using UNSW-NB15 Dataset: Stacking Machine Learning Based Approach", In 2022 International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE), (pp. 1-6). IEEE , February 2022.
- [22] Rosay, A., Cheval, E., Carlier, F., & Leroux, P. , "Network intrusion detection: A comprehensive analysis of CIC-IDS2017", In 8th International Conference on Information Systems Security and Privacy (pp. 25-36). SCITEPRESS-Science and Technology Publications , February 2022.
- [23] Otoum, Y., Wan, Y., & Nayak, A. , "Transfer learning-driven intrusion detection for Internet of Vehicles (IoV)", In 2022 International Wireless Communications and Mobile Computing (IWCMC) (pp. 342-347). IEEE, 2022, May .
- [24] Abd El-Rady, A., Osama, H., Sadik, R., & El Badwy, H. , "Network Intrusion Detection CNN Model for Realistic Network Attacks Based on Network Traffic Classification", In 2023 40th National Radio Science Conference (NRSC) (Vol. 1, pp. 167-178). IEEE, 2022, May.
- [25] Padmavathi, B., & Muthukumar, B. , " A deep recursively learning LSTM model to improve cyber security Botnet attack intrusion detection", *International Journal of Modeling, Simulation, and Scientific Computing*, 14(02), 2341018,2023.
- [26] Kasongo, S.M., Sun, Y. , "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset", *J Big Data* 7, 105,2020.
- [27] Hadeel Alazzam, Ahmad Sharieh, Khair Eddin Sabri, , " A feature selection algorithm for intrusion detection system based on (Pigeon Inspired Optimizer)", *Expert Systems with Applications*, Volume 148,113249,ISSN 0957-4174,2020.
- [28] B.VenkataRamana, K Chandra Mouli, Aileni Eenaja, , "Network Intrusion Detection By SVM & ANN With Feature Selection", *International Journal of Creative Research Thoughts (IJCRT)*, Volume 8, Issue 6 June 2020.



- [29] Kamalov, F., Moussa, S., Zgheib, R., & Mashaal, O. , " Feature selection for intrusion detection systems",In 2020 13th international symposium on computational intelligence and design (ISCID) (pp. 265-269). IEEE,2020.
- [30] Jaw, E., & Wang, X. , "Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach", *Symmetry*, 13(10), 1764,2021.
- [31] Muhsen, A. R., Jumaa, G. G., AL Bakri, N. F., & Sadiq, A. T. , " Feature Selection Strategy for Network Intrusion Detection System (NIDS) Using Meerkat Clan Algorithm", *International Journal of Interactive Mobile Technologies*, 15(16),2021.
- [32] Farhan, R. I., Maalood, A. T., & Hassan, N. , " Hybrid Feature Selection Approach to Improve the Deep Neural Network on New Flow-Based Dataset for NIDS", *Wasit Journal of Computer and Mathematics Science*, 66-83,2021.
- [33] Mojtahedi, A., Sorouri, F., Souha, A. N., Molazadeh, A., & Mehr, S. S. , "Feature selection-based intrusion detection system using genetic whale optimization algorithm and sample-based classification", *arXiv preprint arXiv:2201.00584*,2022.
- [34] Mohammad, A. H. , "Intrusion Detection Using a New Hybrid Feature Selection Model", *Intelligent Automation & Soft Computing*, 30(1),2021.
- [35] Li, X., Yi, P., Wei, W., Jiang, Y., & Tian, L. , " LNNLS-KH: a feature selection method for network intrusion detection",*Security and Communication Networks*, 1-2, 2021.
- [36] Ali, A., Shaikat, S., Tayyab, M., Khan, M. A., Khan, J. S., & Ahmad, J. , " Network intrusion detection leveraging machine learning and feature selection", In 2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET) (pp. 49-53). IEEE,2020.
- [37] Zhang, Y., Zhang, H., & Zhang, B. , "An effective ensemble automatic feature selection method for network intrusion detection", *Information*, 13(7), 314,2022.
- [38] Ren, K., Zeng, Y., Cao, Z., & Zhang, Y. , "ID-RDRL: a deep reinforcement learning-based feature selection intrusion detection model",*Scientific Reports*, 12(1), 15370,2022.
- [39] Patil, D. R., & Pattewar, T. M. , "Majority Voting and Feature Selection Based Network Intrusion Detection System", *EAI Endorsed Transactions on Scalable Information Systems*, 9(6), e6-e6,2022.
- [40] Fauzi, J., Lim, C., & Budiarto, E. , "Efficient model intrusion detection system through feature selection based on decision tree algorithm", *resmilitaris*, 13(2), 231-240,2023.