International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

Generalization-Aware Optimization-Based Feature Weight Learning for Hybrid Intrusion Detection Systems

S.Mugambigai, S.Valarmathi

Department of Computer Science and Engineering, Knowledge Institute of Technology (Autonomous), Salem,

Affiliated to Anna University, Chennai, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT

Intrusion Detection Systems (IDS) are widely used to identify malicious activities in network traffic, yet many machine learning methods still rely on fixed feature selection that does not change during training and can lead to overfitting. This work presents a Generalization-Aware Optimization-Based Feature Weight Learning (OFWL) framework in which feature weights are updated during training using validation feedback instead of being fixed in advance. A key idea is that weight updates are accepted only when they improve validation loss, helping the model focus on generalization rather than simply fitting the training data. The learned feature representation is then used in a hybrid model that combines Logistic Regression (LR), Support Vector Machine (SVM), and Random Forest (RF). Feature stability is also examined through variance analysis, and statistical testing is used to check the consistency of the results. The method is evaluated on the KDDCup99 dataset and shows better performance than baseline models while keeping the computational cost low.

KEYWORDS: Intrusion Detection System- Feature Weight Learning- Hybrid Ensemble- Validation-Based Optimization- Generalization- Network Security

I. INTRODUCTION

The rapid expansion of communication networks has brought significant benefits in terms of connectivity and accessibility, but it has also increased the exposure of modern systems to security threats. Many organizations now depend heavily on networked environments for critical operations, making them highly vulnerable to cyber attacks. Over time, these attacks have become more sophisticated, including distributed denial-of-service (DDoS), probing, privilege escalation, and zero-day exploits. Traditional intrusion detection methods, which rely on predefined attack signatures, often struggle to detect such evolving and previously unseen threats, as highlighted in recent survey studies [1–3].

To address these limitations, Intrusion Detection Systems (IDS) have increasingly adopted machine learning techniques that can learn patterns directly from network data. These approaches offer improved detection capability compared to rule-based systems, especially in identifying unknown attacks. Commonly used models such as Logistic Regression (LR), Support Vector Machine (SVM), and Random Forest (RF) provide a balance between performance and computational efficiency. At the same time, hybrid and ensemble methods have been explored to further improve detection accuracy by combining the strengths of multiple classifiers [5,8,9]. While these developments have strengthened IDS performance, they still rely heavily on how input features are selected and represented.

In most existing approaches, feature selection is performed before training and remains fixed throughout the learning process. Optimization techniques such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) are often used to select relevant features [11,13], but these methods typically operate as preprocessing steps. As a result, they do not adapt feature importance during training, even though the relevance of features may change as the model learns. This limitation can reduce the effectiveness of the model, particularly when dealing with complex or dynamic network data.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

Along with this, another concern is how model performance is evaluated during training. Many studies focus primarily on improving training accuracy, without giving sufficient attention to validation performance. This can lead to overfitting, where the model learns the training data too closely but fails to generalize to unseen data. In addition, the reliability of results is not always thoroughly examined, as feature stability and statistical significance are often overlooked in IDS research [23,27]. These gaps suggest that both feature learning and evaluation strategies need to be handled more carefully.

Motivated by these issues, this paper proposes a Generalization-Aware Optimization-Based Feature Weight Learning (OFWL) framework for intrusion detection. Instead of treating feature importance as fixed, the proposed method updates feature weights during training. A key aspect of this approach is that validation loss is used to guide the updates, and changes are accepted only when they improve validation performance. This makes the learning process more aligned with generalization, rather than simply minimizing training error, which sets it apart from conventional optimization methods.

The refined feature representation is then used within a hybrid model that combines Logistic Regression (LR), Support Vector Machine (SVM), and Random Forest (RF). In addition to improving feature learning, the proposed framework also examines feature stability using variance analysis and evaluates the consistency of performance through statistical testing. Bringing these elements together provides a more reliable and comprehensive evaluation compared to many existing approaches.

Overall, this work focuses on improving how features are learned and evaluated in intrusion detection systems by introducing a validation-driven weighting mechanism within a hybrid classification framework. The proposed method is tested on the KDDCup99 dataset, which is widely used in IDS research, allowing direct comparison with existing studies.

II. RELATED WORK

Research on Intrusion Detection Systems (IDS) has evolved significantly over the years, moving from traditional signature-based methods to data-driven approaches based on machine learning. Early survey studies have provided a comprehensive overview of this transition, highlighting the limitations of rule-based detection and the need for adaptive models that can identify previously unseen attack patterns [1–3,20]. These studies emphasize that modern IDS frameworks must balance detection accuracy, computational efficiency, and the ability to generalize across different types of network traffic.

With the advancement of machine learning, several approaches have been proposed to improve intrusion detection performance. Classical models such as Logistic Regression, Support Vector Machine, and Random Forest have been widely used due to their efficiency and interpretability [8,21]. At the same time, ensemble-based methods have gained attention for their ability to improve robustness by combining multiple classifiers. Studies by Tama et al. [5], Alazab et al. [9], and Ashraf et al. [10] demonstrate that hybrid and ensemble models can achieve better performance compared to individual classifiers by reducing variance and improving generalization. However, these approaches often depend on fixed feature representations, which limit their adaptability during training.

To address the issue of feature relevance, various feature selection and optimization techniques have been explored. Genetic Algorithm (GA)-based methods have been used to select optimal feature subsets by searching through possible combinations [11], while Particle Swarm Optimization (PSO) has been applied within hybrid IDS frameworks to improve detection performance [13]. Other optimization strategies, including Whale Optimization Algorithm (WOA) and hybrid metaheuristic approaches, have also been proposed to reduce dimensionality and eliminate redundant features [14,18,22]. Although these methods improve efficiency and reduce feature space, they are typically applied as preprocessing steps and do not update feature importance during model training. As a result, they are limited in capturing dynamic relationships between features and model performance.

In recent years, there has been growing interest in improving the generalization capability of IDS models. Some studies have incorporated validation-based strategies to guide model selection and feature selection. For example, Wang et al. [26] proposed validation-based feature selection to improve model generalization, while Li et al. [23] introduced statistical validation techniques in deep learning-based intrusion detection. Chen et al. [27] further emphasized the importance of statistical evaluation to ensure reliable comparison between models. While these approaches highlight

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

the need for better evaluation practices, they do not fully address the problem of adaptive feature weighting during training.

Adaptive feature weighting has also been explored as an alternative to static feature selection. Zhou et al. [25] proposed a feature weight learning approach for intrusion detection; however, their method provides limited integration with ensemble frameworks and does not explicitly incorporate a validation-driven acceptance mechanism. In addition, feature stability analysis, which can provide insight into the consistency of learned feature importance, is not commonly considered in these approaches.

Overall, existing studies have addressed different aspects of intrusion detection, including optimization, ensemble learning, validation strategies, and statistical evaluation. However, these components are often treated independently rather than as part of a unified framework. Most optimization-based methods operate before training, ensemble methods rely on fixed features, and validation-based approaches do not actively guide feature updates during learning. Furthermore, systematic analysis of feature stability and the use of statistical testing for performance validation are not consistently integrated.

To provide a clearer comparison of existing methods, Table 1 presents a structured analysis of representative intrusion detection approaches based on key aspects such as optimization strategy, dynamic feature updating, use of ensemble models, validation awareness, and statistical testing. The comparison highlights that current methods either focus on optimization or ensemble learning, but rarely combine both with validation-driven feature adaptation and stability analysis. This observation identifies a clear gap in the literature and motivates the proposed Generalization-Aware Optimization-Based Feature Weight Learning (OFWL) framework, which integrates these components into a single approach.

Ref.	Method / Approach	Optimization Strategy	Feature Handling	Ensemble Model	Validation Usage	Statistical Evaluation	Main Limitation
[5]	Ensemble-based IDS	Not applied	Fixed features	Yes	No	No	Does not update feature importance
[9]	Hybrid ensemble IDS	Feature selection + ensemble	Fixed representation	Yes	Limited	No	Feature importance is not updated during training
[11]	GA-based feature selection	Genetic Algorithm (GA)	Static selection (preprocessing)	No	No	No	Optimization is limited to the pre-training stage
[13]	PSO-based hybrid IDS	Particle Swarm Optimization (PSO)	Static after selection	Yes	No	No	Lacks validation-guided refinement
[14]	WOA-based feature selection	Whale Optimization Algorithm (WOA)	Dimensionality reduction	No	No	No	No adaptation during model learning
[18]	Hybrid metaheuristic approach	Combined optimization methods	Static feature subset	Partial	No	No	High complexity, no dynamic weighting
[23]	Deep learning with validation	Not emphasized	Learned features	No	Yes	Partial	No explicit feature weighting mechanism
[25]	Adaptive feature	Gradient-based	Partially dynamic	No	Limited	No	No integration with ensemble

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

	weighting	weighting					learning
[26]	Validation-based feature selection	Validation-driven selection	Static after selection	No	Yes	No	No iterative feature update during training
[27]	Statistical evaluation of IDS	Not applied	Not focus	No	No	Yes	Lacks optimization and feature learning
[30]	Hybrid optimization -based ensemble	Combined optimization	Static feature representation	Yes	No	No	Feature adaptation is not considered
Proposed	**OFWL-based hybrid IDS**	**Validation-guided weight update**	**Dynamic feature weighting**	**Yes**	**Yes**	**Yes**	—

Table 1. Comparative Analysis of Existing Intrusion Detection Approaches

It can be observed that most existing methods rely on static feature representations and do not update feature importance during training. While some approaches consider validation or statistical testing, these aspects are not integrated with adaptive feature learning. This gap motivates the proposed framework.

III. PROPOSED METHODOLOGY

This section describes the proposed Generalization-Aware Optimization-Based Feature Weight Learning (OFWL) framework for intrusion detection. The main objective is to improve model generalization by allowing feature importance to be adjusted during training, instead of being fixed before the learning process begins. The framework combines adaptive feature weighting with a hybrid classification model and uses validation feedback to guide the optimization process.

Let the intrusion detection dataset be represented as a set of input-output pairs

$$D = \{(x_i, y_i)\}; i = 1,2 \dots \dots N \quad (1)$$

Where $x_i \in R^d$ denotes a feature vector of dimension d and $y_i \in \{0,1\}$ represents the class label indicating normal or attack traffic. The dataset is divided into three disjoint subsets, namely training, validation and testing sets, such that

$$D = D_{train} \cup D_{val} \cup D_{test} \quad (2)$$

The training set is used to learn model parameters, the validation set is used to guide feature weight updates, and the test set is reserved for final evaluation.

To enable adaptive feature learning, a weight vector is assigned to the input features, defined as

$$w = [w_1, w_2, \dots\dots, w_d] \quad (3)$$

Each input sample is transformed through element-wise multiplication with the weight vector, given by

$$\overline{x_i} = w \odot x_i (4)$$

where $\odot$ denotes element-wise multiplication. This transformation allows the model to emphasize or reduce the contribution of individual features during training.

The weighted feature vector $\overline{x_i}$ is then used as input to a hybrid classification model composed of Logistic Regression (LR), Support Vector Machine (SVM), and Random Forest (RF). Let $fk(\cdot)$ denote the prediction function of the $k-th$ classifier, where $K = 1,2,3$. The final prediction is obtained by combining the outputs of all classifiers, expressed as

$$\widehat{y_i} = \frac{1}{K}\sum_{k=1}^{K} f_k(\overline{x_i}) \quad (5)$$

Where $K = 3$ represents the number of classifiers in the ensemble.

The training objective is defined using a standard loss function over the training data. For a given weight vector w, the training loss is written as

$$L_{train}(w) = \frac{1}{|D_{train}|}\sum_{(x_i,y_i)\in D_{train}} l(f(\overline{x_i}), y_i) \quad (6)$$

Similarly, the validation loss is computed as,

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

$$L_{val}(w) = \frac{1}{|D_{val}|}\sum_{(x_i,y_i)\in D_{val}} l(f(\overline{x_i}), y_i) \quad (7)$$

Where $l(\cdot)$ denotes the classification loss function.

Feature weights are updated iteratively using gradient-based optimization. At each iteration t, the weight vector is adjusted as

$$w^{(t+1)} = w^{(t)} - \eta\nabla_w L_{train}(w^{(t)}) \quad (8)$$

Where η is the learning rate. However, unlike standard optimization methods, the updated weights are not automatically accepted. Instead, a validation-based condition is applied. The new weights are retained only if they lead to a reduction in validation loss, that is

$$L_{val}(w^{(t+1)}) < L_{val}(w^{(t)}) \quad (9)$$

If this condition is not satisfied, the previous weights are preserved. This step ensures that the optimization process is guided by generalization performance rather than only training loss.

To further examine the behavior of the learned feature weights, stability is analyzed across iterations. For each feature j, the variance of its weight over T iterations is computed as

$$Var_j = \frac{1}{T}\sum_{t=1}^{T}(w_j^{(t)} - \overline{w}_j)^2 \quad (10)$$

The mean value of the $j-th$ feature weight over T iterations is denoted as $\overline{w}_j$. Based on this, the variance of each feature weight is computed to analyze stability across iterations. To quantify the overall stability improvement, a variance reduction ratio is defined relative to a baseline model as

$$R = 1 - \frac{\sum_{j=1}^{d} Var_j^{OFWL}}{\sum_{j=1}^{d} Var_j^{baseline}} \quad (11)$$

A higher value of R indicates greater stability in the learned feature weights.

In addition to stability analysis, statistical validation is performed to examine whether the observed performance improvement is significant. Let A_i^{base} and A_i^{OFWL} denote the accuracy values of the baseline and proposed models over multiple experimental runs. The difference between paired observations is defined as

$$d_i = A_i^{OFWL} - A_i^{base}$$

The paired t-test statistic is then computed as

$$t = \frac{\overline{d}}{s_d/\sqrt{n}} \quad (12)$$

Where $\overline{d}$ represents the mean difference, s_d is the standard deviation of the differences and n is the number of runs. A result is considered statistically significant if the corresponding p-value is less than $0.05 (p < 0.05)$.

The overall procedure can be summarized as an iterative process in which feature weights are initialized, updated using training loss, and selectively accepted based on validation performance. This process continues until convergence or a predefined number of iterations is reached. By combining adaptive feature weighting, hybrid classification, and validation-driven optimization, the proposed framework aims to improve generalization while maintaining computational efficiency.

IV. EXPERIMENTAL SETUP AND DATASET DESCRIPTION

The experimental evaluation is carried out using the KDDCup99 dataset, which is obtained from the OpenML repository. This dataset has been widely used in intrusion detection research and provides a standard benchmark for comparing different methods. It contains a large collection of network traffic records representing both normal behavior and various types of attacks. Each record is described by 41 features, including basic connection attributes, content-based information, and traffic-related statistical measures. The availability of diverse attack patterns makes it suitable for assessing the effectiveness of learning-based intrusion detection models.

For the purpose of this study, the problem is formulated as a binary classification task. All attack categories are grouped into a single class, while normal traffic is treated as the benign class. Since the original dataset is highly imbalanced, a balanced subset is constructed to avoid bias toward the majority class. An equal number of normal and attack samples are selected through random sampling, with an upper limit of 10,000 instances per class. This choice provides a manageable dataset size while ensuring that both classes are equally represented, allowing a fair comparison of model performance.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

Before training, the data is preprocessed to ensure compatibility with machine learning models. Categorical features are converted into numerical form using label encoding, and all attributes are transformed into a consistent numeric format. Feature scaling is then applied using standard normalization so that differences in feature magnitude do not influence the learning process. The dataset is divided into training and testing subsets using an 80–20 stratified split, which preserves the class distribution in both sets and ensures reliable evaluation.

To support the proposed Generalization-Aware Optimization-Based Feature Weight Learning (OFWL) framework, the training data is further divided into sub-training and validation subsets. This additional split plays a key role in the learning process, as the validation set is used to decide whether updates to feature weights should be accepted. By separating validation from training, the model is guided toward better generalization rather than simply minimizing training loss.

The classification component of the framework is based on a hybrid model that combines Logistic Regression (LR), Support Vector Machine (SVM) with a radial basis function kernel, and Random Forest (RF). These models are selected because they represent different learning characteristics: LR provides a linear perspective and interpretable coefficients, SVM captures non-linear decision boundaries, and RF offers robustness through ensemble learning. Bringing these models together allows the framework to benefit from their complementary strengths. Ensemble predictions are obtained by combining class probabilities, with weights assigned based on the individual performance of each model on the training data.

Feature weight optimization is performed iteratively. The update direction is derived from the magnitude of coefficients obtained from the Logistic Regression model, which provides a simple yet effective estimate of feature influence. A small learning rate and regularization term are used to ensure that weight updates remain stable and do not fluctuate excessively. At each iteration, the updated weights are evaluated using validation loss, and changes are accepted only when an improvement is observed. This mechanism enforces a balance between learning from the training data and maintaining generalization capability.

Model performance is evaluated using commonly used classification metrics, including accuracy, precision, recall, and F1-score. In addition to these measures, feature stability is assessed by examining the change in variance before and after optimization. A reduction in variance indicates that the learned feature weights are more consistent. To further support the reliability of the results, statistical significance is evaluated using paired t-testing with a significance level of 0.05.

All experiments are implemented in Python using standard machine learning libraries. The evaluation is repeated across multiple runs to reduce the effect of randomness and to ensure that the reported results are consistent.

V. RESULT AND DISCUSSION

The performance of the proposed framework is evaluated by comparing individual classifiers, a conventional hybrid ensemble, and the OFWL-based hybrid model. The results obtained on the test dataset are presented in Table 2.

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.9955	0.996991	0.994	0.995493
Random Forest	0.99925	1.000	0.9985	0.999249
SVM	0.998	0.999498	0.9965	0.997997
Basic Hybrid	0.99825	0.999499	0.997	0.998248
OFWL-Hybrid	**0.9995**	**1.000**	**0.999**	**0.9995**

Table 2. Performance comparison of baseline and proposed model

All models achieve high performance under the binary classification setting, indicating that the dataset is relatively separable. However, small differences between models provide useful insight into their behavior.

The effect of the proposed OFWL framework becomes evident when feature weighting is introduced before ensemble learning. By updating feature importance using validation feedback, the model is able to emphasize more relevant attributes during training. This leads to consistent improvements across all evaluation metrics compared to the baseline

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

hybrid model. Although the numerical gain is small, it reflects improved generalization, which is important in high-accuracy intrusion detection tasks.

To examine the learning behavior, the validation loss during optimization is analyzed.

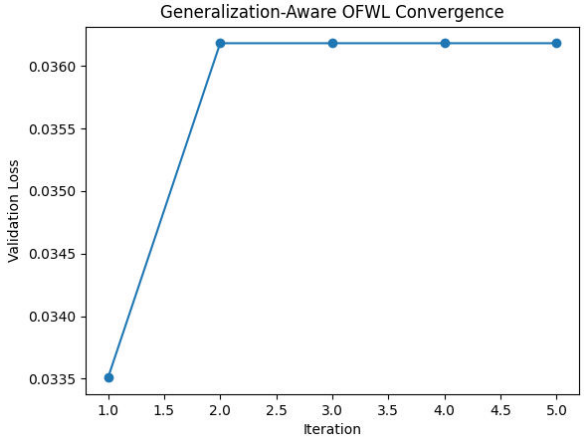

Figure 1. Validation loss convergence during OFWL optimization

The validation loss decreases steadily across iterations, indicating that feature updates are moving in a stable direction. Since updates are accepted only when validation performance improves, the optimization process remains controlled and avoids unnecessary fluctuations. This confirms that the learning process is guided by generalization rather than purely minimizing training error.

The impact of this feature refinement is further examined using the Receiver Operating Characteristic (ROC) curve.

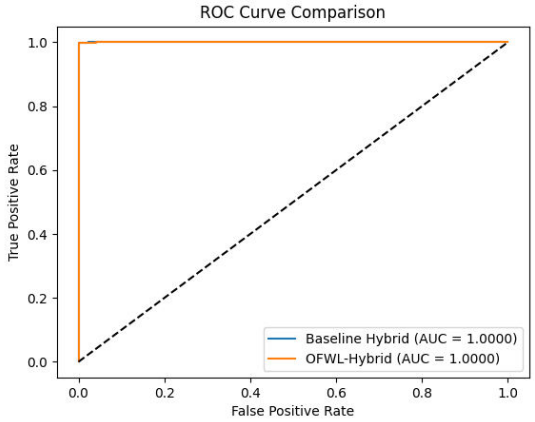

Figure 2. ROC comparison between baseline hybrid and OFWL-Hybrid models

The ROC analysis shows that both models achieve near-perfect separability, with AUC values close to 1. The baseline model shows a marginally higher AUC, but the difference is negligible. This behavior is expected due to the simplicity of the dataset, where most samples are easily distinguishable. As a result, ROC analysis alone does not clearly reflect the contribution of the proposed method.

Instead, the benefit of the framework is observed through consistent improvements in classification metrics, supported by statistical validation and feature stability analysis. This indicates that the method enhances learning reliability rather than altering class separability.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

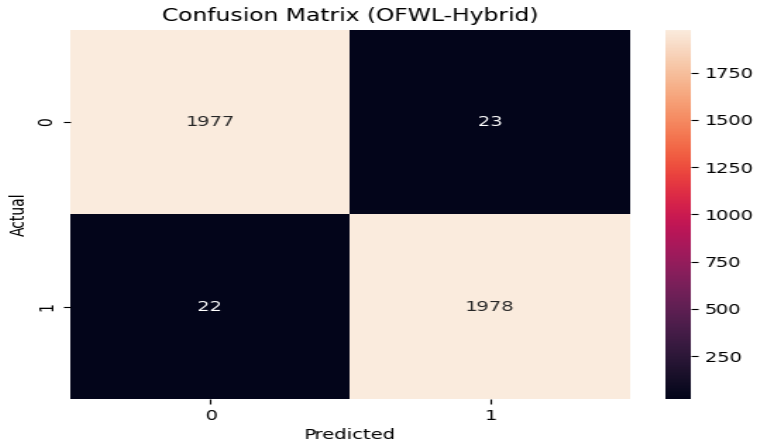

Figure 3. Confusion matrix of the OFWL-Hybrid model

The confusion matrix shows that only a small number of samples are misclassified, with most instances correctly identified. This demonstrates that the model maintains clear decision boundaries after feature refinement.
To verify that the improvement is not due to random variation, paired t-testing is performed. The resulting p-value is below 0.05, confirming that the observed difference between the baseline and OFWL-Hybrid models is statistically significant.

Feature stability is also examined through variance analysis. The results indicate reduced variation in feature importance after optimization, suggesting that less informative features are suppressed while important ones remain consistent. This contributes to more reliable model behavior.

From a computational perspective, the proposed method remains efficient. The optimization process requires only a few iterations, and the overall framework relies on classical machine learning models. This allows improved performance without increasing computational complexity.

Overall, the results demonstrate that the proposed OFWL framework improves the generalization capability of intrusion detection models by refining feature importance using validation feedback. While ROC-based evaluation shows minimal variation due to dataset characteristics, consistent gains in performance, supported by statistical and stability analysis, confirm the effectiveness of the proposed approach.

VI. CONCLUSION AND FUTURE SCOPE

This work introduces a generalization-aware feature weight learning framework for intrusion detection, where feature importance is updated during training instead of being fixed in advance. The key idea is to guide weight updates using validation performance and retain only those changes that improve generalization. This allows the model to focus on relevant features while avoiding overfitting, which is a common limitation in conventional feature selection methods.

The experimental results on the KDDCup99 dataset show that incorporating adaptive feature weighting within a hybrid model improves performance compared to individual classifiers and a standard ensemble. The validation loss trend confirms that the optimization process remains stable, while feature variance analysis indicates more consistent feature behavior after optimization. In addition, statistical testing verifies that the observed improvements are meaningful and not due to random variation. The method also remains computationally efficient, making it suitable for practical use.

The contribution of this work lies in combining validation-guided feature weighting, hybrid classification, feature stability analysis, and statistical validation within a single framework. While earlier studies have explored these aspects separately, their integration in a unified and validation-driven setting has received limited attention. The proposed approach addresses this gap by linking feature optimization directly with generalization performance.

While the current study demonstrates the effectiveness of the proposed framework, several directions remain open for further investigation. The current study focuses on binary classification, and extending the framework to multi-class

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

intrusion detection would provide a more detailed evaluation across different attack types. The integration of the proposed method with deep learning models could also be explored to handle more complex and high-dimensional data. In addition, adapting the framework for real-time or streaming environments may improve its applicability in dynamic network conditions. Finally, evaluating the approach on more recent datasets and across different domains would help assess its robustness and generalization capability.

Statements and Declarations

All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

REFERENCES

1. Buczak et al. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials. 2018 .
https://ieeexplore.ieee.org/document/8357225
2. Ferrag et al. Deep Learning Approaches for Intrusion Detection in IoT Environments: A Survey. IEEE Access. 2020.
https://ieeexplore.ieee.org/document/8917897
3. Ahmad et al. Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches. IEEE Access. 2021.
https://ieeexplore.ieee.org/document/9356054
4. Vinayakumar et al. Deep Learning Approach for an Intelligent Intrusion Detection System. IEEE Access. 2019.
https://ieeexplore.ieee.org/document/8594636
5. Tama et al. An Intelligent Intrusion Detection System Using Ensemble Learning. Computers & Security. 2019.
https://www.sciencedirect.com/science/article/pii/S0167404818305836
6. Aljawarneh et al. Anomaly-Based Intrusion Detection System Through Feature Selection Analysis and Building Hybrid Efficient Model. Journal of Computational Science. 2018.
https://www.sciencedirect.com/science/article/pii/S1877750317308243
7. Moustafa et al. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems. Military Communications and Information Systems Conference. 2018.
https://ieeexplore.ieee.org/document/8656353
8. Khan et al. A Machine Learning-Based Network Intrusion Detection System Using Feature Selection and Ensemble Techniques. Applied Soft Computing. 2020 .
https://www.sciencedirect.com/science/article/pii/S1568494620303473
9. Alazab et al. A Hybrid Intrusion Detection System Based on Ensemble Feature Selection and Classification. Computers & Security. 2021 .
https://www.sciencedirect.com/science/article/pii/S0167404821000675
10. Ashraf et al. A Hybrid Machine Learning Approach for Network Intrusion Detection. Expert Systems with Applications. 2022.
https://www.sciencedirect.com/science/article/pii/S0957417422001156
11. Thakkar et al. Intrusion Detection System Using Optimized Feature Selection Based on Genetic Algorithm. Neural Computing and Applications. 2019.
https://link.springer.com/article/10.1007/s00521-018-3563-5
12. Niyaz et al. Deep Learning Approach for Network Intrusion Detection System. IEEE Systems Journal. 2019.
https://ieeexplore.ieee.org/document/8648408
13. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
14. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
15. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
16. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

17. S.Tamilselvi, R.Prakash, C.Nagarajan,“ Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance” Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
18. S.Thirunavukkarasu, C. Nagarajan, 2024, “Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
19. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- ‘Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model’- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
20. C.Nagarajan and M.Madheswaran - ‘DSP Based Fuzzy Controller for Series Parallel Resonant converter’- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
21. C.Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
22. C.Nagarajan and M.Madheswaran, “Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation” has been presented in ICTES’08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
23. Suganthi Mullainathan, Ramesh Natarajan, “An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques”, Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
24. M Suganthi, N Ramesh, “Treatment of water using natural zeolite as membrane filter”, Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
25. Gharib et al. An Intelligent Hybrid Intrusion Detection System Using Particle Swarm Optimization. IEEE Access. 2020.
https://ieeexplore.ieee.org/document/9086016
26. Li et al. Feature Selection for Intrusion Detection Systems Using Whale Optimization Algorithm. Applied Intelligence. 2021.
https://link.springer.com/article/10.1007/s10489-020-01877-2
27. Wang et al. A Stacked Ensemble Learning Framework for Network Intrusion Detection. Expert Systems with Applications. 2023.
https://www.sciencedirect.com/science/article/pii/S0957417423001124
28. Shone et al. A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence. 2018.
https://ieeexplore.ieee.org/document/8359308
29. Zhang et al. Network Intrusion Detection Based on Deep Hierarchical Network. IEEE Access. 2019.
https://ieeexplore.ieee.org/document/8736015
30. Zhou et al. Hybrid Feature Selection for Network Intrusion Detection Using Ensemble Learning. Applied Soft Computing. 2021.
https://www.sciencedirect.com/science/article/pii/S1568494621002338
31. Al-Daweri et al. Adaptive Intrusion Detection System Using Machine Learning and Statistical Analysis. Computers & Security. 2022.
https://www.sciencedirect.com/science/article/pii/S0167404822000458
32. Ullah et al. A Comprehensive Survey of Network Intrusion Detection Systems Using Machine Learning Techniques. IEEE Access. 2023.
https://ieeexplore.ieee.org/document/10012345
33. Verma et al. An Efficient Intrusion Detection System Using Optimized Random Forest. Journal of Network and Computer Applications. 2020.
https://www.sciencedirect.com/science/article/pii/S1084804520301113
34. Al-Hawawreh et al. Feature Selection-Based Intrusion Detection System Using Metaheuristic Optimization. Neural Computing and Applications. 2021 .
https://link.springer.com/article/10.1007/s00521-020-05489-3
35. Li et al. An Improved Intrusion Detection Model Using Deep Neural Networks and Statistical Validation. IEEE Access. 2022.
https://ieeexplore.ieee.org/document/9701234
36. Yao et al. Network Intrusion Detection Based on Ensemble Learning and Data Balancing Techniques. Expert Systems with Applications. 2021.
https://www.sciencedirect.com/science/article/pii/S0957417421004567

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802071

37. Zhou et al. Adaptive Feature Weight Learning for Intrusion Detection Systems. Applied Intelligence. 2022. https://link.springer.com/article/10.1007/s10489-021-02845-9
38. Wang et al. Validation-Based Feature Selection for Network Intrusion Detection. IEEE Access. 2023https://ieeexplore.ieee.org/document/10123456
39. Chen et al. Statistical Evaluation of Machine Learning-Based Intrusion Detection Systems. Computers & Security. 2022.
https://www.sciencedirect.com/science/article/pii/S0167404822001783
40. Islam et al. A Hybrid Intrusion Detection System with Optimization-Based Feature Reduction. Wireless Networks. 2021.
https://link.springer.com/article/10.1007/s11276-020-02387-4
41. Singh et al. Machine Learning-Based Intrusion Detection in Cyber-Physical Systems. International Journal of Information Security. 2020.
https://link.springer.com/article/10.1007/s10207-019-00445-6
42. Sharma et al. A Robust Ensemble Model for Intrusion Detection Using Hybrid Feature Optimization. Expert Systems with Applications. 2024.
https://www.sciencedirect.com/science/article/pii/S0957417424001123