International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

AN OPTIMIZED IRLS-SVM FRAMEWORK FOR IOT CYBERSECURITY: VULNERABILITY ASSESSMENT AND THREAT DETECTION

Ranjeeta Pandhare[1], Dr. Jaydeep B. Patil[2,*], and Dr. Sangram T. Patil[3]

[1]Research Scholar, Department of Computer Science & Engineering,

D. Y. Patil Agriculture and Technical University, Talsande, Maharashtra, India;

&

Assistant Professor, Department of Computer Science & Engineering,

Kolhapur Institute of Technology's College of Engineering, Kolhapur, Maharashtra, India.
Email: ranjeeta.pandhare@gmail.com

[2,*]Associate Professor, Department of Computer Science & Engineering, D. Y. Patil Agriculture & Technical University, Talsande, Maharashtra, India.

Email: jaydeeppatil@dyp-atu.org

[3]Associate Dean, Department of Computer Science & Engineering,

D. Y. Patil Agriculture & Technical University, Talsande, Maharashtra, India.

Email: sangrampatil@dyp-atu.org

Abstract

The increasing deployment of Internet of Things (IoT) systems in smart cities, healthcare, and industrial environments has intensified cybersecurity challenges due to large-scale and evolving attack patterns. Traditional security mechanisms are often ineffective in detecting sophisticated and unknown threats. This paper presents an optimized machine learning–based framework for vulnerability assessment and threat detection in IoT networks. The proposed approach employs Z-score normalization for data preprocessing, L1-norm–based Mayfly Optimization (LNMFO) for selecting optimal features, and an Iteratively Reweighted Least Squares–based Support Vector Machine (IRLS-SVM) for robust classification. The optimization-driven feature selection reduces dimensionality and improves computational efficiency, while the IRLS mechanism enhances resilience to noise and outliers. Experimental evaluation on the BoTNeTIoT and HIKARI-2021 datasets demonstrates that the proposed framework achieves superior performance, with detection accuracy reaching 99%, outperforming existing intrusion detection methods. The results highlight the effectiveness of the proposed model for reliable IoT cybersecurity applications.

Index Terms - Internet of Things, Cybersecurity, Intrusion Detection System, Feature Selection, IRLS-SVM, Mayfly Optimization, Machine Learning

Received: December 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

I. INTRODUCTION

The Internet of Things (IoT) has rapidly evolved as a core technology enabling smart cities, healthcare monitoring, industrial automation, smart grids, and intelligent transportation systems. By interconnecting heterogeneous devices such as sensors, actuators, and embedded systems, IoT facilitates real-time data acquisition, automation, and intelligent decision-making. Recent advancements in wireless communication and cloud-based platforms have further accelerated large-scale IoT deployments [19], [15]. However, the massive connectivity and decentralized nature of IoT systems have introduced serious cybersecurity challenges.

IoT environments are inherently vulnerable due to limited computational resources, lack of standardized security mechanisms, and continuous data transmission over public networks. These constraints make IoT networks attractive targets for cyber-attacks such as Distributed Denial of Service (DDoS), botnets, malware propagation, spoofing, and data tampering [20], [14]. Largescale attacks exploiting compromised IoT devices can disrupt critical services, compromise sensitive data, and cause significant economic and operational damage [9].

Conventional security solutions, including rule-based firewalls and signature-based intrusion detection systems (IDS), are insufficient to address modern IoT threats. These approaches rely heavily on predefined attack signatures and struggle to detect zero-day and evolving attacks, resulting in high false alarm rates and poor adaptability [16], [13]. As IoT traffic continues to grow in volume and complexity, there is a strong need for intelligent and adaptive security mechanisms.

Machine learning (ML)–based intrusion detection systems have emerged as effective alternatives by enabling automated analysis of large-scale network traffic and identification of anomalous behavior [8], [4]. ML models can learn complex patterns and relationships from historical data, allowing them to detect both known and previously unseen attacks. Despite these advantages, many ML-based IDS suffer from challenges such as high-dimensional feature spaces, noisy data, redundant attributes, and misclassification, which negatively impact detection accuracy and computational efficiency [6], [2].

To overcome these limitations, recent research has focused on optimization-based feature selection and robust classification techniques. Feature selection reduces dimensionality and eliminates irrelevant attributes, improving model generalization and execution speed [3]. Similarly, advanced classifiers that are resilient to noise and outliers have demonstrated improved detection performance in complex IoT environments [11]. Bio-inspired optimization algorithms, such as Mayfly Optimization, have shown promising results in selecting optimal feature subsets for cybersecurity applications [17].

Motivated by these observations, this paper proposes a hybrid optimization-driven intrusion detection framework for IoT cybersecurity. The framework integrates data preprocessing, feature selection, and robust classification to enhance detection accuracy and reliability across diverse attack scenarios.

The main contributions of this work are summarized as follows:

- Z-score normalization is employed to preprocess IoT traffic data and ensure feature consistency.

Received: December 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- An L1-norm–based Mayfly Optimization algorithm is used to select optimal and discriminative features, reducing dimensionality and computational cost.
- An Iteratively Reweighted Least Squares–based Support Vector Machine (IRLS-SVM) classifier is applied to improve robustness against noise and outliers.
- Extensive experiments are conducted on benchmark BoTNeTIoT and HIKARI-2021 datasets to evaluate performance across multiple attack types.

II. RELATED WORK

Recent advancements in Internet of Things (IoT) security have led to the development of various machine learning (ML) and deep learning (DL)–based intrusion detection systems. Existing research primarily focuses on detecting network anomalies, botnet activities, and denial-of-service attacks using supervised, unsupervised, and hybrid learning models. While several approaches demonstrate improved detection accuracy, many of them suffer from challenges such as high computational complexity, sensitivity to noisy and imbalanced data, limited feature optimization, and poor generalization to unseen attacks.

To address these limitations, recent studies have explored optimization-assisted feature selection techniques and robust classifiers to enhance detection reliability and efficiency. A comparative summary of prominent research works related to IoT intrusion detection, along with their methodologies and limitations, is presented in Table I. This analysis highlights existing research gaps and motivates the need for an optimized framework integrating effective feature selection and robust classification, as proposed in this study.

Table I presents a comparative summary of important research works on IoT intrusion detection using machine learning and deep learning techniques, highlighting their methodologies, datasets, and key limitations.

A. Research Gap

The review of existing literature on IoT intrusion detection systems reveals several unresolved challenges. Although machine learning and deep learning–based approaches have demonstrated improved detection performance, many existing models rely on high-dimensional feature spaces, resulting in increased computational complexity and degraded generalization. Several studies employ deep learning architectures that require extensive training time and high computational resources, limiting their applicability in resource-constrained IoT environments.

Moreover, most existing intrusion detection frameworks do not adequately address the impact of noisy, redundant, and imbalanced data, which leads to misclassification and high false alarm rates. Feature selection is often overlooked or performed using conventional techniques that fail to identify the most discriminative attributes. Additionally, many classifiers lack robustness against outliers and dynamic attack behaviors, reducing detection reliability in real-world IoT scenarios. These limitations highlight the need for an optimized and lightweight intrusion detection framework that integrates effective feature selection with a robust classification mechanism.

Received: December 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

B. Objectives

Based on the identified research gaps, the primary objectives of this study are:

- To develop an optimized and lightweight intrusion detection framework for IoT environments by integrating effective data preprocessing, feature selection, and classification.
- To design an L1-norm–based Mayfly Optimization algorithm for selecting optimal and discriminative features, thereby reducing dimensionality and computational complexity.
- To implement an Iteratively Reweighted Least Squares–based Support Vector Machine (IRLS-SVM) classifier to enhance detection accuracy and robustness against noisy and imbalanced IoT data.

TABLE I: Summary of Related Work on IoT Intrusion Detection

Paper Title	**Author(s) and Year**	**Methodology**	**Key Limitations**
Towards the Development of Realistic Botnet Dataset in the IoT for Network Forensic Analytics	Koroniotis *et al.* (2019)	Statistical feature extraction with ML classifiers	High class imbalance and limited real-time applicability
Use of Machine Learning Algorithms for Designing Efficient Cyber Security Solutions	Soni and Bhushan (2019)	Traditional ML-based IDS models	Feature redundancy and scalability issues
Artificial Intelligence and Cybersecurity: Past, Presence, and Future	Truong *et al.* (2020)	Survey of AI techniques in cybersecurity	Lack of experimental validation
Cybersecurity Data Science: An Overview from Machine Learning Perspective	Sarker *et al.* (2020)	ML-driven cybersecurity framework	Absenceof optimization-based feature selection
Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining	Rekha *et al.* (2020)	Data mining and ML-based IDS	High false positive rates
A Survey on Machine Learning Techniques for Cyber Security in the Last Decade	Shaukat *et al.* (2020)	Comparative analysis of ML algorithms	Computational overhead in complex models
Selection of Effective Machine Learning Algorithm and Bot-IoT Attacks Traffic Identification	Shafiq *et al.* (2020)	ML-based Bot-IoT attack de-tection	Limited generalization to unseen attacks

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Computational Intelligence Enabled Cybersecurity for the Internet of Things	Zhao *et al.* (2020)	Computational intelligence models for IoT security	Resource-intensive implementations
IoT Security: Botnet Detection in IoT Using Machine Learning	Pokhrel *et al.* (2021)	Supervised ML classifiers	Poorperformance against zero-day attacks
AI-DrivenCybersecurity: An Overview,Security Intelligence Modeling and Research Directions	Sarker *et al.* (2021)	AI-based cybersecurity framework	Lack of robust classification models
MapReduce Based Intelligent Model for Intrusion Detection Using Machine Learning Technique	Asif *et al.* (2021)	Distributed ML-based IDS	High computational complexity
An Intelligent Tree-Based Intrusion Detection Model for Cyber Security	Al-Omari *et al.* (2021)	Decision tree-based IDS	Sensitivity to noisy and imbalanced data
A Real-Time Sequential Deep Extreme Learning Machine Cybersecurity IDS	Haider *et al.* (2021)	Deep Extreme Learning Ma-chine	Parameter sensitivity and tuning complexity
Detecting Cybersecurity Attacks in IoT Using Artificial Intelligence Methods: A Systematic Review	Abdullahi *et al.* (2022)	Systematic review of AI-based IDS	Lack of comparative experimental results
A Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things	Alkhudaydi *et al.* (2023)	Deep learning-based IDS	High training cost and computational complexity

III. PROPOSED METHODOLOGY

The proposed intrusion detection framework integrates data preprocessing, optimization-based feature selection, and robust classification to accurately identify normal and malicious IoT traffic. The overall workflow is designed to reduce dimensionality, handle noisy data, and improve classification reliability in IoT environments.

Received: December 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A. System Architecture

The overall system architecture of the proposed intrusion detection framework is illustrated in Fig. 1. The architecture is designed to systematically process IoT network traffic through four major stages: data collection, data preprocessing, feature selection, and classification. Benchmark IoT intrusion datasets, namely BoTNeTIoT and HIKARI-2021, are utilized to train and evaluate the proposed model.

As shown in Fig. 1, the data collection stage gathers raw network traffic records from IoT environments, which are subsequently divided into training and testing datasets. In the data preprocessing stage, Z-score normalization is applied to both training and testing data to ensure uniform feature scaling and to eliminate bias caused by differing feature ranges. This step improves model convergence and stability.

Following preprocessing, an optimization-driven feature selection stage is employed. The L1-norm–based Mayfly Optimization (LNMFO) algorithm is used to identify the most discriminative and relevant features while removing redundant and irrelevant attributes. This reduces dimensionality and computational overhead without compromising classification performance.

Finally, the selected features are fed into an Iteratively Reweighted Least Squares–based Support Vector Machine (IRLSSVM) classifier. The IRLS-SVM assigns adaptive weights to training samples, enhancing robustness against noise and outliers.

The classification stage outputs the final decision by categorizing network traffic into *Normal* or *Vulnerable* classes. The integrated architecture ensures efficient, accurate, and reliable intrusion detection in IoT environments.

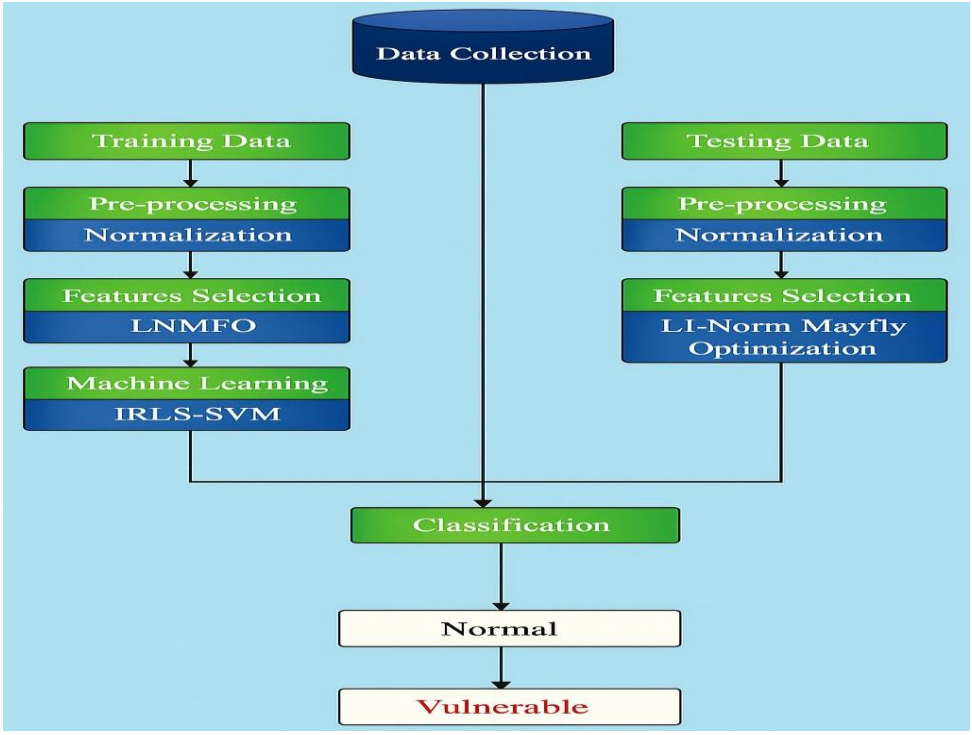

Fig. 1: System architecture of the proposed LNMFO–IRLS-SVM–based IoT intrusion detection framework.

Received: December 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

B. Data Preprocessing

IoT traffic data often contain features with varying scales and distributions, which can adversely affect learning algorithms. To address this issue, Z-score normalization is applied to standardize the feature values. The normalized value Z of a feature is computed as:

$$Z = \frac{X - \mu}{\sigma} \tag{1}$$

where X represents the original feature value, μ denotes the mean of the feature, and σ is the corresponding standard deviation. This normalization ensures that all features contribute equally during model training and improves convergence stability.

C. Feature Selection Using L1-Norm Mayfly Optimization

Following preprocessing, feature selection is performed to reduce dimensionality and eliminate redundant attributes. The proposed framework employs an L1-norm–based Mayfly Optimization (LNMFO) algorithm, which is a bio-inspired optimization technique that simulates the social and mating behavior of mayflies.

In the Mayfly Optimization algorithm, each candidate solution represents a feature subset encoded as a position vector in a d-dimensional search space. The velocity and position of each mayfly are updated iteratively to explore and exploit the search space. The fitness function is defined to maximize classification accuracy while minimizing the number of selected features, expressed as:

$$\min F = \alpha(1 - Acc) + \beta\|\mathbf{w}\|_1 \tag{2}$$

where Acc denotes the classification accuracy, $\mathbf{w}$ represents the feature weight vector, $\|\cdot\|_1$ is the L1-norm promoting sparsity, and α and β are control parameters balancing accuracy and feature reduction. The velocity update for male mayflies is given by:

$$\mathbf{v}_i^{t+1} = g\mathbf{v}_i^t + c_1 r_1(\mathbf{p}_i - \mathbf{x}_i^t) + c_2 r_2(\mathbf{g} - \mathbf{x}_i^t) \tag{3}$$

where $\mathbf{v}_i^t$ and $\mathbf{x}_i^t$ denote the velocity and position of the i-th mayfly at iteration t, $\mathbf{p}_i$ is the personal best position, $\mathbf{g}$ is the global best position, g is the inertia factor, c_1 and c_2 are acceleration coefficients, and $r_1, r_2 \in [0,1]$ are random numbers.

By incorporating the L1-norm in the fitness evaluation, the algorithm effectively selects a compact and informative feature subset, reducing computational complexity and improving classification performance.

D. Classification Using IRLS-SVM

The selected features are classified using an Iteratively Reweighted Least Squares–based Support Vector Machine (IRLSSVM). Unlike standard SVM, the IRLS-SVM assigns adaptive weights to training samples, reducing the influence of noisy data and outliers.

The SVM optimization problem is formulated as:

N

$$\min_{\mathbf{w},b} \frac{1}{2}\|\mathbf{w}\|^2 + C\sum_{i=1}\rho(\ _i) \quad \_e \tag{4}$$

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

where **w** is the weight vector, b is the bias term, C is the penalty parameter, e_i represents the classification error for the i-th sample, and $\rho(\cdot)$ is a robust loss function.

In the IRLS framework, the optimization is solved iteratively by updating sample weights:

$$w_i^{(t+1)} = \frac{1}{|e_i^{(t)}| + \epsilon} \tag{5}$$

where $w_i^{(t+1)}$ is the updated weight at iteration $t+1$, $e_i^{(t)}$ is the error at iteration t, and ϵ is a small constant to avoid division by zero.

This iterative reweighting process improves robustness against noisy and imbalanced IoT data. The final decision function of the IRLS-SVM classifier is expressed as:

$$f(\mathbf{x}) = \text{sign}\left(\sum_{i=1}^{N} \alpha_i y_i K(\mathbf{x}_i, \mathbf{x}) + b\right) \tag{6}$$

where α_i are Lagrange multipliers, y_i are class labels, and $K(\cdot,\cdot)$ is the Gaussian kernel function.

Through the integration of optimization-driven feature selection and robust classification, the proposed framework effectively detects normal and malicious IoT traffic with high accuracy and reliability.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed LNMFO–IRLS-SVM framework is implemented using Python and evaluated on two benchmark IoT intrusion datasets, namely BoTNeTIoT and HIKARI-2021. The experiments are conducted to assess the effectiveness of the proposed model in detecting malicious and vulnerable traffic patterns. The performance of the proposed approach is compared with existing techniques such as SMOTE, ECASP, CRPF, and conventional SVM. Evaluation metrics include accuracy, precision, recall, F1-score, detection rate, and Receiver Operating Characteristic (ROC) analysis.

A. Performance matrix

The performance of the proposed intrusion detection framework is evaluated using multiple standard metrics, including accuracy, precision, recall, F1-score, detection rate, and Receiver Operating Characteristic (ROC) analysis. As summarized in Table II, accuracy represents the overall correctness of the classification model, while precision and recall indicate the framework's ability to minimize false positives and correctly detect malicious traffic, respectively. The F1-score provides a balanced assessment by jointly considering precision and recall, making it particularly suitable for evaluating performance on imbalanced IoT intrusion datasets.

In addition, the detection rate measures the capability of the proposed model to successfully identify attack instances, which is critical for real-world IoT security applications. The high detection rate achieved by the proposed LNMFO–IRLSSVM framework demonstrates its effectiveness in capturing diverse attack patterns. Furthermore, ROC analysis evaluates the trade-off between true positive and false positive rates, and the high area under the ROC curve (AUC) indicates strong discriminative capability. Overall, the consistently high values across

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

all performance metrics confirm the robustness, reliability, and generalization ability of the proposed framework compared to existing intrusion detection approaches.

The proposed LNMFO–IRLS-SVM framework achieves consistently high values across all metrics, with accuracy, precision, recall, and F1-score reaching up to 99%, outperforming SMOTE, CRPF, and conventional SVM-based approaches shown in Figure 2. In addition, the high detection rate demonstrates the effectiveness of the proposed model in identifying attack instances, while the ROC analysis with an AUC close to 0.99 confirms strong discrimination capability between normal and vulnerable traffic. These results highlight the robustness, reliability, and superior generalization performance of the proposed framework for IoT intrusion detection.

TABLE II: Comparison of Accuracy, Precision, Recall, and F1-score

Method	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-score (%)**
Proposed LNMFO–IRLS-SVM	99.0	96.0	94.0	93.0
SVM	92.0	78.0	78.0	82.0
CRPF	85.0	82.0	82.0	80.0
SMOTE	82.0	80.0	80.0	74.0

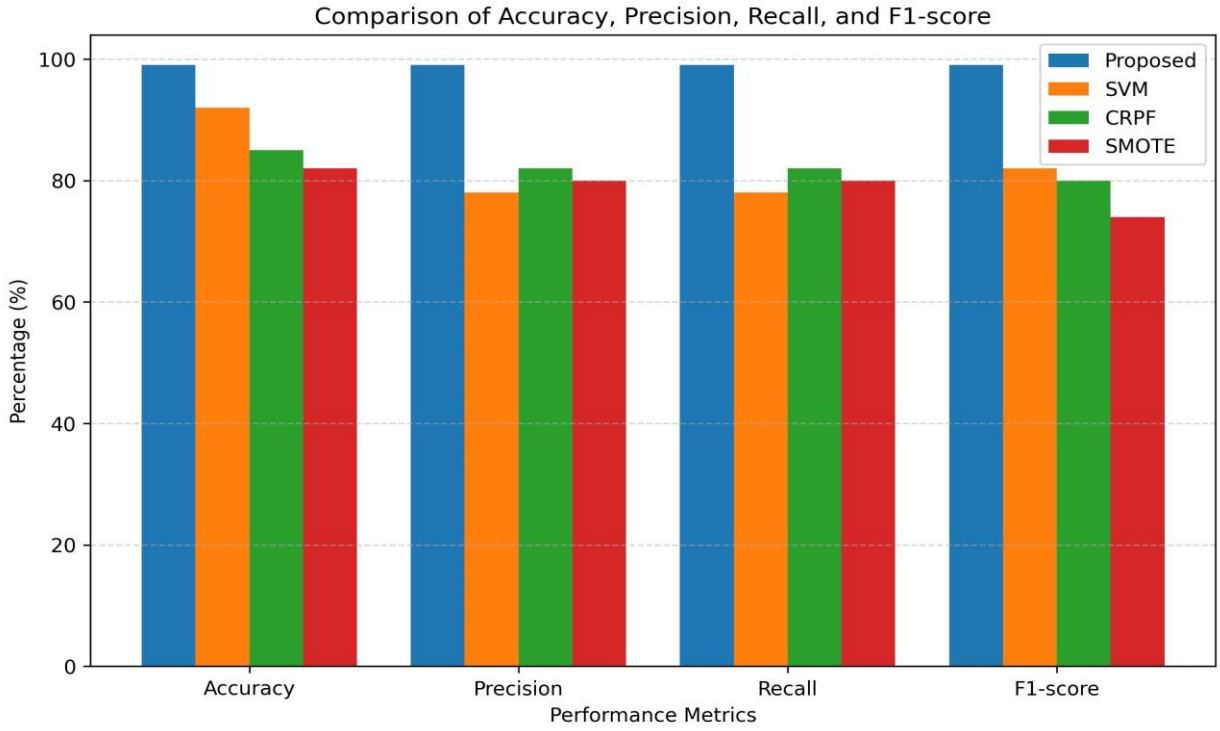

Fig. 2: Comparison of accuracy, precision, recall, and F1-score for the proposed LNMFO–IRLS-SVM framework and existing methods.

Received: December 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

B. Detection Rate Analysis

Detection rate evaluates the capability of the model to correctly identify attack instances. Fig. 3 depicts the detection rate comparison for different methods. The proposed framework achieves a detection rate close to 99% for BoTNeTIoT and nearly 100% for the HIKARI-2021 dataset, confirming its effectiveness in identifying diverse attack scenarios.

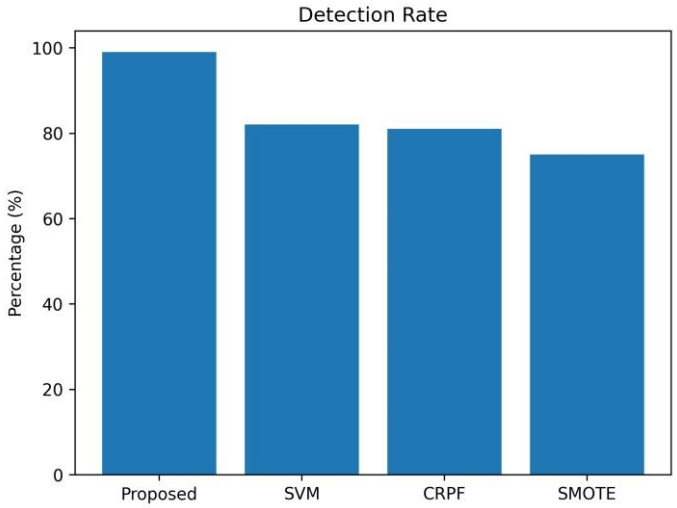

Fig. 3: Detection rate comparison on BoTNeTIoT and HIKARI-2021 datasets.

C. ROC Curve and AUC Analysis

The ROC curve illustrates the trade-off between true positive rate and false positive rate. Fig. 4 shows the ROC curves for the proposed model on both datasets. The Area Under the Curve (AUC) value of approximately 0.99 indicates excellent discrimination capability and robustness of the proposed intrusion detection framework.

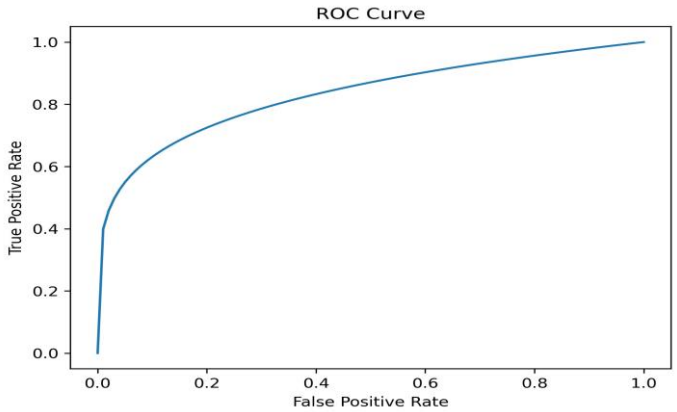

Fig. 4: ROC curves of the proposed LNMFO–IRLS-SVM framework.

D. Attack-wise Performance Analysis

To further analyze detection effectiveness, attack-wise performance is evaluated. Fig. 5 presents detection rates for different attack categories. In the BoTNeTIoT dataset, high detection rates are observed for DDoS and botnet attacks, while in the HIKARI-2021 dataset,

International Journal of Applied Mathematics
Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the proposed model demonstrates strong performance in detecting DoS and tampering attacks. These results validate the generalization ability of the proposed framework across multiple attack types.

Overall, the experimental results confirm that the integration of L1-norm–based Mayfly Optimization and IRLS-SVM significantly enhances intrusion detection accuracy, robustness, and reliability when compared to existing state-of-the-art methods.

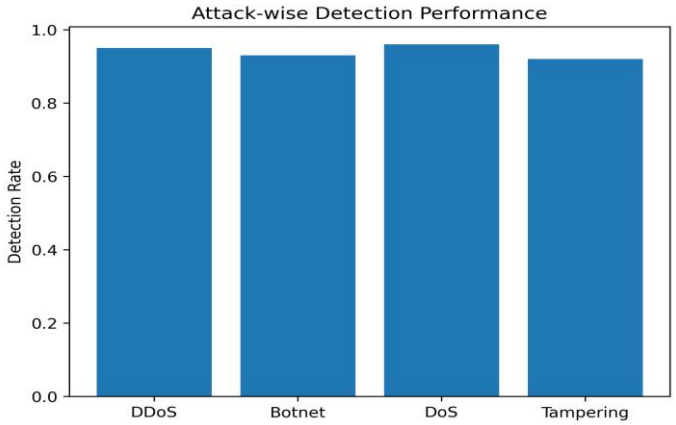

Fig. 5: Attack-wise detection performance on BoTNeTIoT and HIKARI-2021 datasets.

V. CONCLUSION

This paper presented an optimized machine learning–based intrusion detection framework for IoT cybersecurity, integrating Z-score normalization, L1-norm–based Mayfly Optimization for feature selection, and an Iteratively Reweighted Least Squares

Support Vector Machine (IRLS-SVM) for classification. The proposed framework effectively addresses key challenges in IoT security, including high-dimensional data, noise, and class imbalance. Experimental evaluations conducted on the BoTNeTIoT and HIKARI-2021 datasets demonstrated that the proposed LNMFO–IRLS-SVM approach achieves superior performance across multiple metrics, including accuracy, precision, recall, F1-score, detection rate, and ROC-AUC, with accuracy reaching up to 99%. The results confirm the robustness, reliability, and generalization capability of the proposed framework in detecting diverse IoT cyber-attacks.

Future Scope

Future work will focus on extending the proposed framework for real-time intrusion detection in large-scale IoT environments by integrating streaming data processing mechanisms. Additionally, the model can be enhanced to handle zero-day and advanced persistent threats through online learning and adaptive optimization strategies. Further investigation will also explore lightweight deployment on edge and fog computing platforms, as well as the incorporation of explainable artificial intelligence techniques to improve model transparency and trustworthiness.

Received: December 08, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

REFERENCES

[1] D. Kwon, R.-M. Neagu, P. Rasakonda, J. T. Ryu, and J. Kim, "Evaluating unbalanced network data for attack detection," in *Proc. Systems and Network Telemetry and Analytics*, 2023.

[2] A. Raza, K. Munir, M. S. Almutairi, and R. Sehar, "Novel class probability features for optimizing network attack detection with machine learning," *IEEE Access*, 2023.

[3] O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, "A deep learning methodology for predicting cybersecurity attacks on the Internet of Things," *Information*, vol. 14, no. 10, p. 550, 2023.

[4] M. Abdullahi *et al.*, "Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, 2022.

[5] R. Fernandes and N. Lopes, "Network intrusion detection packet classification with the HIKARI-2021 dataset," in *Proc. 10th Int. Symp. Digital Forensics and Security (ISDFS)*, IEEE, 2022.

[6] B. Dash, M. F. Ansari, P. Sharma, and A. Ali, "Threats and opportunities with AI-based cyber security intrusion detection: A review," *Int. J. Software Engineering & Applications*, vol. 13, no. 5, 2022.

[7] P. Rajak, J. Lachure, and R. Doriya, "CNN-LSTM-based IDS on precision farming for IIoT data," in *Proc. IEEE Int. Conf. Cybernetics, Cognition and Machine Learning Applications*, 2022.

[8] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: An overview, security intelligence modeling and research directions," *SN Computer Science*, vol. 2, 2021.

[9] S. Pokhrel, R. Abbas, and B. Aryal, "IoT security: Botnet detection in IoT using machine learning," *arXiv preprint arXiv:2104.02231*, 2021.

[10] M. Al-Omari, M. Rawashdeh, F. Qutaishat, M. Alshira'H, and N. Ababneh, "An intelligent tree-based intrusion detection model for cyber security," *Journal of Network and Systems Management*, vol. 29, 2021.

[11] A. Haider, M. A. Khan, A. Rehman, M. U. Rahman, and H. S. Kim, "A real-time sequential deep extreme learning machine cybersecurity intrusion detection system," *Computers, Materials & Continua*, vol. 66, no. 2, 2021.

[12] M. Asif, S. Abbas, M. A. Khan, A. Fatima, M. A. Khan, and S.-W. Lee, "MapReduce based intelligent model for intrusion detection using machine learning technique," *Journal of King Saud University–Computer and Information Sciences*, 2021.

[13] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020.

Received: December 08, 2025

Volume 38 No. 11s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[14] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[15] S. Zhao, S. Li, L. Qi, and L. D. Xu, "Computational intelligence enabled cybersecurity for the Internet of Things," *IEEE Trans. Emerging Topics in Computational Intelligence*, vol. 4, no. 5, pp. 666–674, 2020.

[16] G. Rekha, S. Malik, A. K. Tyagi, and M. M. Nair, "Intrusion detection in cyber security: Role of machine learning and data mining," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 3, pp. 72–81, 2020.

[17] Z. Gao, J. Zhao, S. Li, and Y. Hu, "The improved mayfly optimization algorithm," *Journal of Physics: Conference Series*, vol. 1684, no. 1, p. 012077, 2020.

[18] I. H. Sarker *et al.*, "Cybersecurity data science: An overview from machine learning perspective," *Journal of Big Data*, vol. 7, 2020.

[19] T. C. Truong *et al.*, "Artificial intelligence and cybersecurity: Past, presence, and future," in *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer, 2020.

[20] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

Received: December 08, 2025