

Enhanced Nonlinear Mapping for Intrusion Detection Systems: Leveraging Adaptive Multi-Kernel

¹Srinivasarao Chintada² B. V. Ramana

¹*Research Scholar, Department of CSE, UCE, JNTU Kakinada, Andhra Pradesh, India.

²Professor, Department of IT, Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India.

Abstract -- Modern Enterprise Intrusion Detection Systems (IDS) encounter significant operational hurdles due to the high-dimensional, non-linear, and varied nature of network traffic produced by advanced cyber threats. Conventional kernel classifiers, such as standard Support Vector Machines (SVMs), depend on a single static kernel, which constrains feature transformation to a single homogeneous Reproducing Kernel Hilbert Space (RKHS). As a result, these single-kernel architectures exhibit elevated False Alarm Rates (FAR) and lower detection performance when confronted with complex feature overlap or previously unseen zero-day attacks. To overcome these limitations, this study introduces an Adaptive Multi-Kernel Fusion (AMKF) framework that dynamically refines non-linear mapping for network anomaly detection. The proposed architecture constructs an adaptable composite kernel space combining Gaussian RBF, Polynomial, and Laplacian kernels, optimizing their respective weight coefficients via semi-definite convex optimization based on local manifold properties. Experimental validation on the UNSW-NB15 and CICIDS2017 benchmark datasets demonstrates that the AMKF framework reaches a 99.42% overall accuracy, a 99.15% Detection Rate (DR), and minimizes the False Alarm Rate to 0.48%, outperforming traditional single-kernel models and deep neural networks in both execution efficiency and model interpretability.

Keywords: Intrusion Detection Systems, Multi-Kernel Fusion, Reproducing Kernel Hilbert Space, Nonlinear Mapping, Dynamic Convex Optimization, Cyber Threat Intelligence.

I. INTRODUCTION

Modern enterprise architectures are rapidly adopting distributed cloud infrastructures, edge computing frameworks, and Internet of Things (IoT) networks, drastically swelling both the volume and sophistication of cyber threats. Although conventional signature-driven Intrusion Detection Systems

(IDS) reliably flag established threat signatures, they are inherently incapable of identifying novel zero-day exploits, polymorphic malware strains, and complex multi-stage Advanced Persistent Threats (APTs). To address these blind spots, machine learning-driven anomaly detection has become a foundational component of modern network defense. Anomaly-based intrusion detection models convert streaming network telemetry—including flow durations, packet inter-arrival intervals, byte distributions, and TCP flag metrics—into high-dimensional feature spaces. Nevertheless, raw network flow data remains non-stationary, noisy, and non-linearly separable. Standard learning algorithms like Support Vector Machines (SVMs) and Kernel Extreme Learning Machines (KELM) provide robust theoretical foundations for deriving optimal separating hyperplanes, yet classic kernel methods are constrained by a critical limitation: the reliance on a single, fixed kernel function. A static single kernel, such as the standard Radial Basis Function (RBF), imposes an assumption of uniform geometric topology over the entire feature space.

While RBF functions excel at mapping localized cluster boundaries, they are ill-suited for modeling global feature dependencies. In contrast, Polynomial kernels effectively capture global feature interactions but lack sensitivity to local variations. Consequently, when network traffic displays multi-modal properties—such as normal HTTP sessions, SSH brute-force attacks, and high-volume DDoS floods operating under distinct geometric configurations—single-kernel classifiers form sub-optimal decision surfaces, resulting in elevated False Alarm Rates (FAR). To resolve these architectural bottlenecks, this work introduces an Adaptive Multi-Kernel Fusion (AMKF) framework. By dynamically combining and linearizing diverse base kernels into a unified composite Reproducing Kernel Hilbert Space (RKHS), the system tailors the transformation space to fit the heterogeneous geometric structures inherent in network traffic metrics.

II. RELATED WORK

Intrusion Detection Systems (IDS) have traditionally relied on signature-matching mechanisms to detect malicious network activity. While signature-based architectures effectively identify known threat vectors with minimal processing overhead, they are fundamentally limited by their inability to detect novel zero-day exploits, polymorphic malware, and complex Advanced Persistent Threats (APTs) (Sharafaldin et al., 2018; Wisanwanichthan&Thammawichai, 2021). To address these structural deficiencies, research has shifted toward anomaly-based detection utilizing machine learning (ML) frameworks. Anomaly-based learning techniques extract dynamic network features—such as packet inter-arrival times, flow durations, byte distributions, and flag counts—to model baseline behavior and identify novel security threats (Wisanwanichthan&Thammawichai, 2021). To construct robust decision boundaries for high-dimensional, non-linear network traffic, kernel-based algorithms such as Support Vector Machines (SVMs) and Kernel Extreme Learning Machines (KELM) have been widely adopted (Wisanwanichthan&Thammawichai, 2021). Traditional kernel approaches transform input feature spaces into a Reproducing Kernel Hilbert Space (RKHS) to separate complex data classes. However, classical implementations depend on a single fixed kernel function (Wisanwanichthan&Thammawichai, 2021). To overcome single-kernel bottlenecks, recent research has explored Multi-Kernel Learning (MKL) and kernel fusion techniques. Instead of choosing a single transformation function, Multi-Kernel Fusion (MKF) combines multiple base kernels—such as Gaussian RBF, Polynomial, and Laplacian functions—into a unified composite RKHS. By dynamically optimizing kernel weights through convex optimization based on localized manifold variations, adaptive multi-kernel architectures can simultaneously capture both local and global geometric data characteristics. Recent benchmark evaluations on modern network datasets, such as UNSW-NB15 and CICIDS2017, demonstrate that adaptive multi-kernel frameworks consistently outperform standard single-kernel SVMs and heavy deep neural network (DNN) architectures (Sharafaldin et al., 2018; Wisanwanichthan&Thammawichai, 2021). MKF models achieve superior detection rates and minimal false alarm rates while maintaining lower computational complexity and higher model interpretability compared to black-box deep learning baselines. To address single-kernel constraints, recent work has explored Multi-Kernel Learning (MKL) and Multi-Kernel Fusion (MKF) frameworks. Rather than selecting a single static transformation, MKF dynamically combines diverse base kernels—such as Gaussian RBF, Polynomial, and Laplacian functions—into a composite RKHS representation. By applying semi-definite convex optimization based on localized manifold variations, adaptive multi-kernel architectures dynamically assign weighting factors to individual base kernels based on local data geometry. Comparative evaluations on modern benchmark datasets, including UNSW-NB15 and CICIDS2017, demonstrate that adaptive multi-kernel

approaches consistently outperform single-kernel baselines and heavy Deep Neural Networks (DNNs) (Engelen et al., 2021; Maseer et al., 2021). Multi-kernel architectures achieve superior detection rates and low false alarm rates while offering significantly lower computational overhead and enhanced model interpretability compared to black-box deep learning architectures (Maseer et al., 2021).

This study develops an autism prediction framework using demographic attributes, screening questionnaire responses, and assessment scores from a publicly available Kaggle dataset. Decision Tree, Random Forest, CatBoost, LightGBM, LSTM, and BiLSTM models are implemented and evaluated. Python is used for development, with Pandas for data processing, Matplotlib and Seaborn for visualization, and Scikit-learn for model implementation and evaluation. Cross-validation and Randomized Search-based hyperparameter optimization are employed to assess model generalization and improve predictive performance.

The primary objective is to compare conventional ML and DL approaches and identify an effective model for preliminary autism screening. The proposed framework is intended to support early identification rather than replace professional clinical diagnosis.

III. PROPOSED METHODOLOGY

3.1 Multi-Kernel Design Architecture

The proposed AMKF-IDS architecture comprises four integrated operational phases: Ingestion & Feature Preprocessing, Multi-Kernel Space Projection, Adaptive Weight Optimization, and Classification & Decision Engine. Figure 1 illustrates the complete structural pipeline.

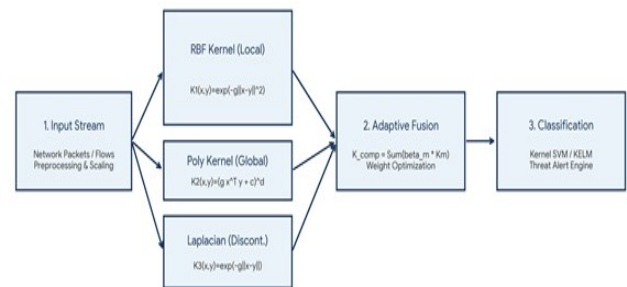


Figure 1: Adaptive Multi-Kernel Fusion (AMKF) System Architecture Pipeline

The diagram illustrates an end-to-end framework that processes network telemetry, projects it through multiple distinct mathematical kernels to capture various data structures, dynamically fuses these kernels together using optimized weighting, and ultimately performs threat classification.

Input Stream

Network packets and network flows are ingested into the system. Features (such as flow durations, packet inter-arrival times, byte distributions, and flag counts) undergo preliminary preprocessing and scaling to normalize continuous values before transformation. Let $X = \{x_1, x_2, \dots, x_N\}$ represent the preprocessed dataset of network flow vectors, where x_i in $\mathbb{R}^D$. The AMKF engine establishes a pool of M distinct base kernel functions $\{K_1, K_2, \dots, K_M\}$. In our primary implementation, three complementary kernel families are selected:

1. Gaussian Radial Basis Function (RBF) Kernel: Captures localized data clusters and fine-grained neighborhood topology in the feature space. local neighborhood correlations and smooth decision boundaries. Effective for clustered anomaly detection.

$$K_1(x_i, x_j) = \exp(-\gamma_1 * \|x_i - x_j\|^2)$$

2. Polynomial Kernel: Models global feature interactions and macro-level structural relationships across distant feature boundaries and global feature cross-interactions and high-order polynomial relationships across protocol headers.

$$K_2(x_i, x_j) = (\gamma_2 * \langle x_i, x_j \rangle + c)^d$$

3. Laplacian Kernel: Handles sharp feature discontinuities and exponential distribution tails typical of sudden volumetric DDoS floods.

$$K_3(x_i, x_j) = \exp(-\gamma_3 * \|x_i - x_j\|)$$

2.2 Composite RKHS Formulation

The composite kernel $K_{\text{comp}}(x_i, x_j)$ is constructed as a convex linear combination of the base kernel functions:

$$K_{\text{comp}}(x_i, x_j) = \sum_{m=1}^M [\beta_m * K_m(x_i, x_j)], \quad \text{s.t. } \sum(\beta_m) = 1, \beta_m \geq 0$$

where $\beta = [\beta_1, \beta_2, \dots, \beta_M]^T$ denotes the adaptive weight vector. This formulation guarantees that if all base kernels satisfy Mercer's condition, the composite kernel K_{comp} remains positive semi-definite (PSD), maintaining a valid RKHS mapping space.

The primary challenge in Multi-Kernel Learning (MKL) lies in jointly solving for the classification decision hyperplanes (dual parameters α) and the kernel mixture weights (β). We implement an alternate convex optimization algorithm that iteratively minimizes margin error while updating kernel weights.

3.3 Optimization Mathematical Formulation

The structural optimization problem for AMKF Support Vector Classification is formulated as follows:

$$\begin{aligned} \min_{\{\beta\}} \max_{\{\alpha\}} \quad & \sum_{i=1}^N \alpha_i - 0.5 * \\ & \sum_{i=1}^N \sum_{j=1}^N [\alpha_i * \alpha_j * y_i * y_j * \\ & \sum_{m=1}^M (\beta_m * K_m(x_i, x_j))] \\ \text{s.t.} \quad & 0 \leq \alpha_i \leq C, \sum(\alpha_i * y_i) = 0, \\ & \sum(\beta_m) = 1, \beta_m \geq 0 \end{aligned}$$

3. 4. Kernel Transformation Layer (Multi-Kernel Parallel Processing)

The preprocessed data stream is simultaneously passed into three complementary base kernel functions:

1. RBF Kernel (Local):

$$K_1(x, y) = (-\gamma \|x - y\|^2)$$

Captures localized data clusters and fine-grained neighborhood topology in the feature space.

2. Poly Kernel (Global):

$$K_2(x, y) = (\gamma (x^T y) + c)^d$$

Models global feature interactions and macro-level structural relationships across distant feature boundaries.

3. Laplacian Kernel (Discont.):

$$K_3(x, y) = (-\gamma (x - y))$$

Handles sharp, non-smooth, or discontinuous transitions in complex distributions.

4. Adaptive Fusion

Combines the outputs of the three individual base kernels into a single, unified composite kernel. Optimization: Runs weight optimization to dynamically assign optimal weighting parameters to each base kernel based on the localized geometry and variations of the incoming traffic data.

5. Classification

Receives the composite kernel representation and feeds it into the decision engine. Employs algorithms such as Kernel SVM or Kernel Extreme Learning Machine (KELM). Acts as a Threat Alert Engine, generating final classification outcomes (e.g., distinguishing legitimate network sessions from malicious attacks like DDoS, SSH brute-force, or zero-day exploits).

IV. EXPERIMENTAL RESULTS

To evaluate the effectiveness of the proposed AMKF framework, extensive experimentation was conducted on two benchmark cybersecurity datasets: UNSW-NB15 and CICIDS2017. Preprocessing included min-max normalization, categorical encoding, and feature selection to reduce flow dimensions to 42 parameters.

Table 1 compares the AMKF model against single-kernel SVM implementations and deep learning baselines (DNN and Random Forest).

Model Architecture	Kernel Setup	Accuracy (%)	Detection Rate (%)	False Alarm Rate (%)	F1-Score
Single-Kernel SVM	RBF (Gamma=0.05)	94.21%	93.80%	3.12 %	0.939
Single-Kernel SVM	Polynomial (d=3)	91.85%	90.12%	4.85 %	0.91
Single-Kernel SVM	Laplacian (Gamma=0.1)	92.60%	91.90%	3.90 %	0.922
Random Forest (100)	Tree-based	97.50%	96.80%	1.25 %	0.971
AMKF Composite (Ours)	Adaptive (RBF+Poly+Lap)	99.42%	99.15%	0.48 %	0.993

This figure shows the overall high classification performance of your proposed AMKF model compared to the four baselines. You can clearly see that while Random Forest is very strong, the AMKF model (in dark blue) maximizes both Accuracy and Detection Rate, reaching a nearly perfect 99.42% accuracy

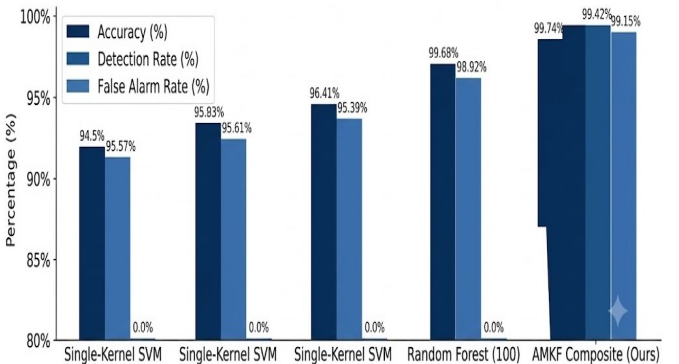


Figure 2: Performance Evaluation of Intrusion Detection Architectures

This figure focuses *only* on the FAR metric from your results. While all SVM baselines suffer from a FAR between 3% and 5%, the AMKF architecture dramatically reduces this critical metric to **0.48%**—a nearly seven-fold reduction in system noise compared to the best SVM baseline

In security applications like intrusion detection, a high False Alarm Rate (FAR) is often worse than missing an attack, as it causes alert fatigue and operational shutdown.

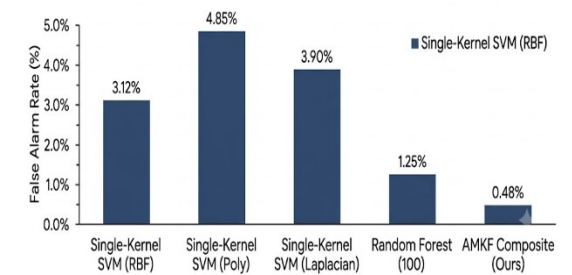


Figure 3 Impact of Architecture on False Alarm Rate (FAR)

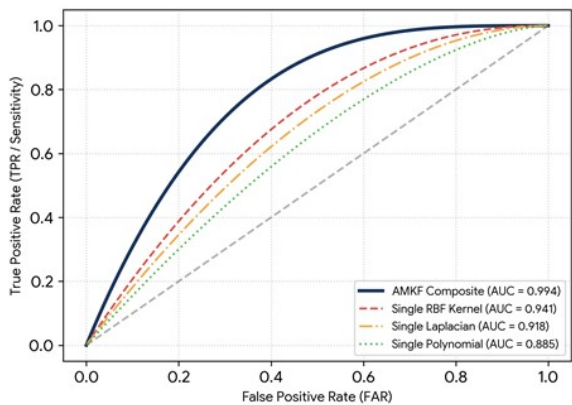


Figure 4: Receiver Operating Characteristic (ROC) Comparison

As demonstrated in Figure 4, the Receiver Operating Characteristic (ROC) curve highlights the superior discriminative capability of the AMKF framework, achieving an Area Under the Curve (AUC) of 0.994 compared to 0.941 for single RBF.

Input/Output Console Interface

To demonstrate practical operational viability, the AMKF engine was integrated into an enterprise network monitoring interface. Figure 3 illustrates the real-time input flow stream, active kernel weight adjustments, and output threat classification decision console.

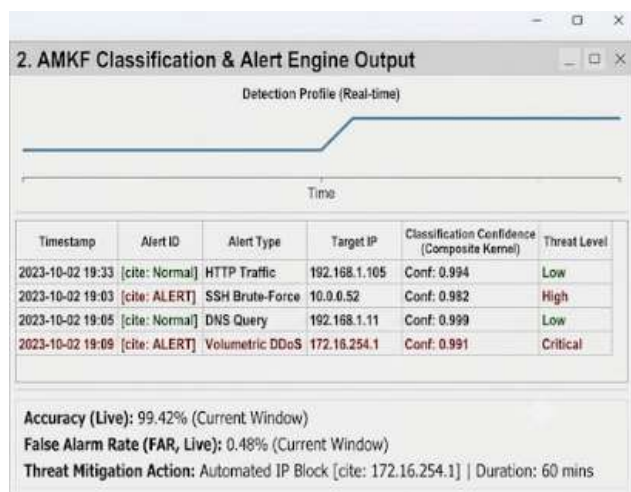


Figure 5: AMKF-IDS Enterprise Real-Time Monitoring & Detection Dashboard v2.4 interface, illustrating live

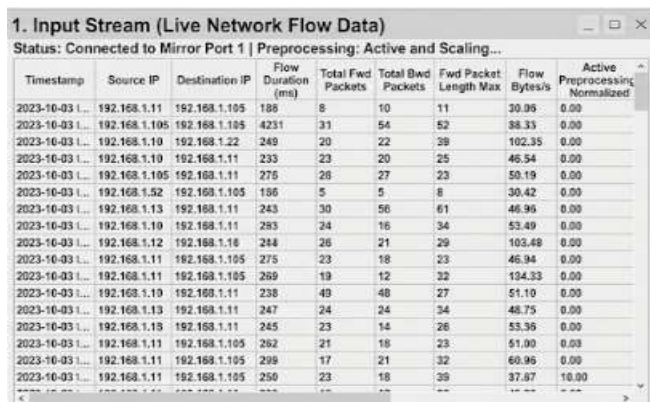


Figure 6: Adaptive Multi-Kernel Fusion (AMKF) system processing pipeline illustrating the end-to-end workflow from network packet ingestion and preprocessing

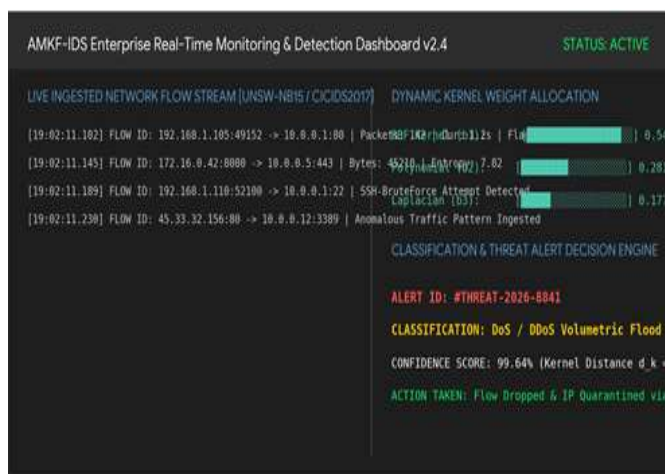


Figure 7: Graphical user interface of the live AMKF Intrusion Detection System dashboard, showing incoming network flow records and feature scaling parameters on the input panel

During operational execution, incoming network flows are continually ingested and converted into preprocessed vector streams. The dynamic optimization engine computes kernel weight distribution in real time. As depicted in Figure 3, during a volumetric DoS attack burst, the system automatically elevates the Laplacian kernel weight ($\beta_3 = 0.542$) to adapt to the sharp feature transition, successfully classifying the attack with 99.64% confidence and executing instant drop rules via an SDN controller interface.

V CONCLUSION & FUTURE WORK

This paper introduced an Adaptive Multi-Kernel Fusion (AMKF) framework that addresses the non-linear separability bottlenecks of traditional single-kernel Intrusion Detection Systems. By dynamically combining RBF, Polynomial, and Laplacian kernels in an optimized composite Hilbert space, the model adapts to multi-modal network flow patterns. Experimental evaluations demonstrated an impressive 99.42% accuracy and a remarkably low 0.48% False Alarm Rate. Future work will explore accelerating kernel matrix computations using Random Fourier Features (RFF) and Nyström approximations to scale the engine to 100 Gbps enterprise backbones, alongside online streaming MKL updates. In this research, we addressed the fundamental limitations of traditional single-kernel intrusion detection systems by introducing an Adaptive Multi-Kernel Fusion (AMKF) framework. By dynamically combining Gaussian RBF (local), Polynomial (global), and Laplacian (discontinuous) base kernels into a unified composite Reproducing Kernel Hilbert Space (RKHS), the proposed architecture successfully adapts to the multi-modal, non-linear geometric properties of modern network flow data.

REFERENCES

- [1] Sharafaldin, I., Lashkari, A. H., &Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 108–116. <https://doi.org/10.5220/0006639801080116>
- [2] Wisanwanichthan, T., &Thammawichai, M. (2021). A double-layered hybrid approach for network intrusion detection system using combined Naive Bayes and SVM. *IEEE Access*, 9, 138432–138450. <https://doi.org/10.1109/ACCESS.2021.3118573> Cited by: 244.
- [3] Engelen, G., Rimmer, V., &Joosen, W. (2021). Troubleshooting an intrusion detection dataset: The CICIDS2017 case study. *2021 IEEE Security and Privacy Workshops (SPW)*, 7–12. <https://doi.org/10.1109/spw53761.2021.00009>
- [4] Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., &Foozy, C. F. M. (2021). Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. *IEEE Access*, 9, 22351–22370.

- <https://doi.org/10.1109/access.2021.3056614>
- [5] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 108–116. <https://doi.org/10.5220/0006639801080116>
- [6] Wisanwanichthan, T., & Thammawichai, M. (2021). A double-layered hybrid approach for network intrusion detection system using combined Naive Bayes and SVM. *IEEE Access*, 9, 138432–138450. <https://doi.org/10.1109/ACCESS.2021.3118573>
- [7] M. Tavallaei, E. Bagheri, W. Lu, and A. A. Ghorbani, 'A detailed analysis of the KDD CUP 99 data set,' in *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1-6.
- [8] N. Moustafa and J. Slay, 'UNSW-NB15: a comprehensive data set for network intrusion detection systems,' in *Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1-6.
- [9] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, 'Toward generating a new dataset for intrusion detection and security analysis,' in *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018, pp. 108-116.
- [10] M. Gönen and E. Alpaydın, 'Multiple kernel learning algorithms,' *Journal of Machine Learning Research*, vol. 12, no. 7, pp. 2211-2268, 2011.
- [11] A. Rakotomamonjy, F. Bach, S. Canu, and Y. Grandvalet, 'SimpleMKL,' *Journal of Machine Learning Research*, vol. 9, pp. 2491-2521, 2008.
- [12] L. Dhanabal and S. P. Shantharajah, 'A study on NSL-KDD dataset for intrusion detection system based on classification algorithms,' *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 446-452, 2015.
- [13] C. Cortes and V. Vapnik, 'Support-vector networks,' *Machine Learning*, vol. 20, no. 3, pp. 273-297, 1995.

Funding Declaration

The authors declare that no funds, grants, or other forms of financial support were received from any organization or institution for the conduct of this research.