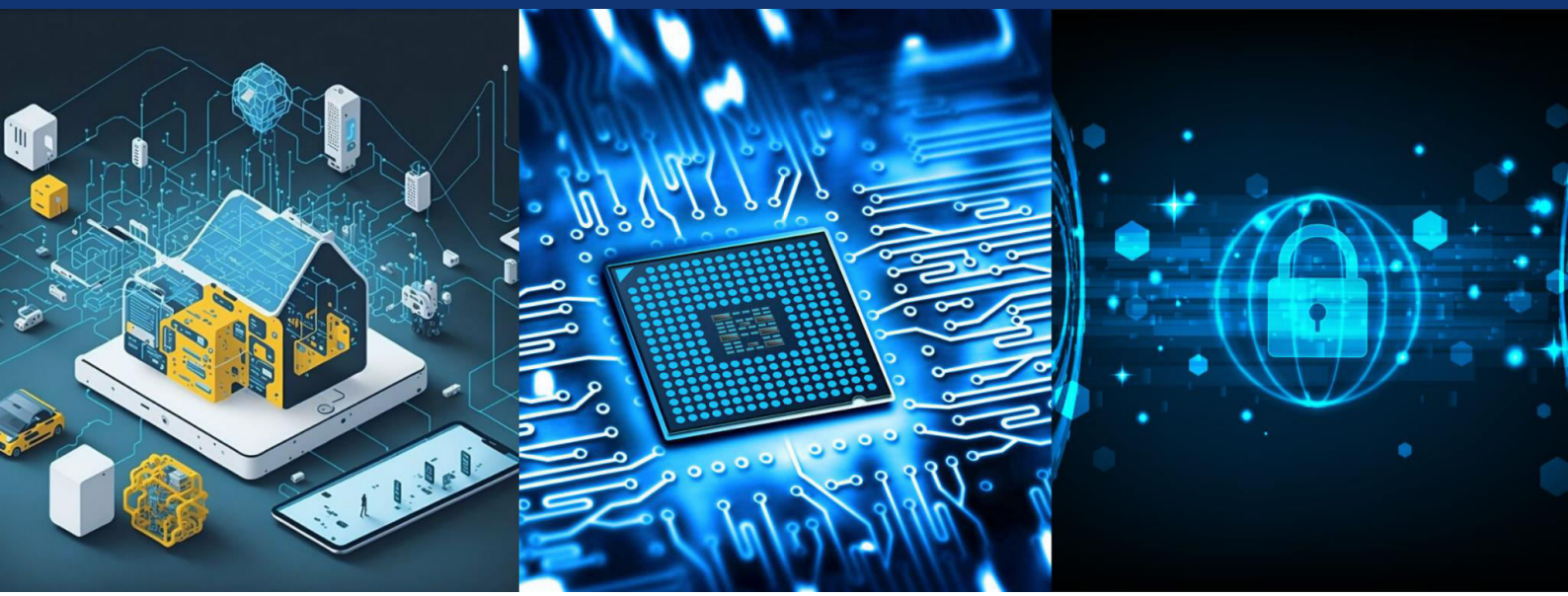
IJIRCCE

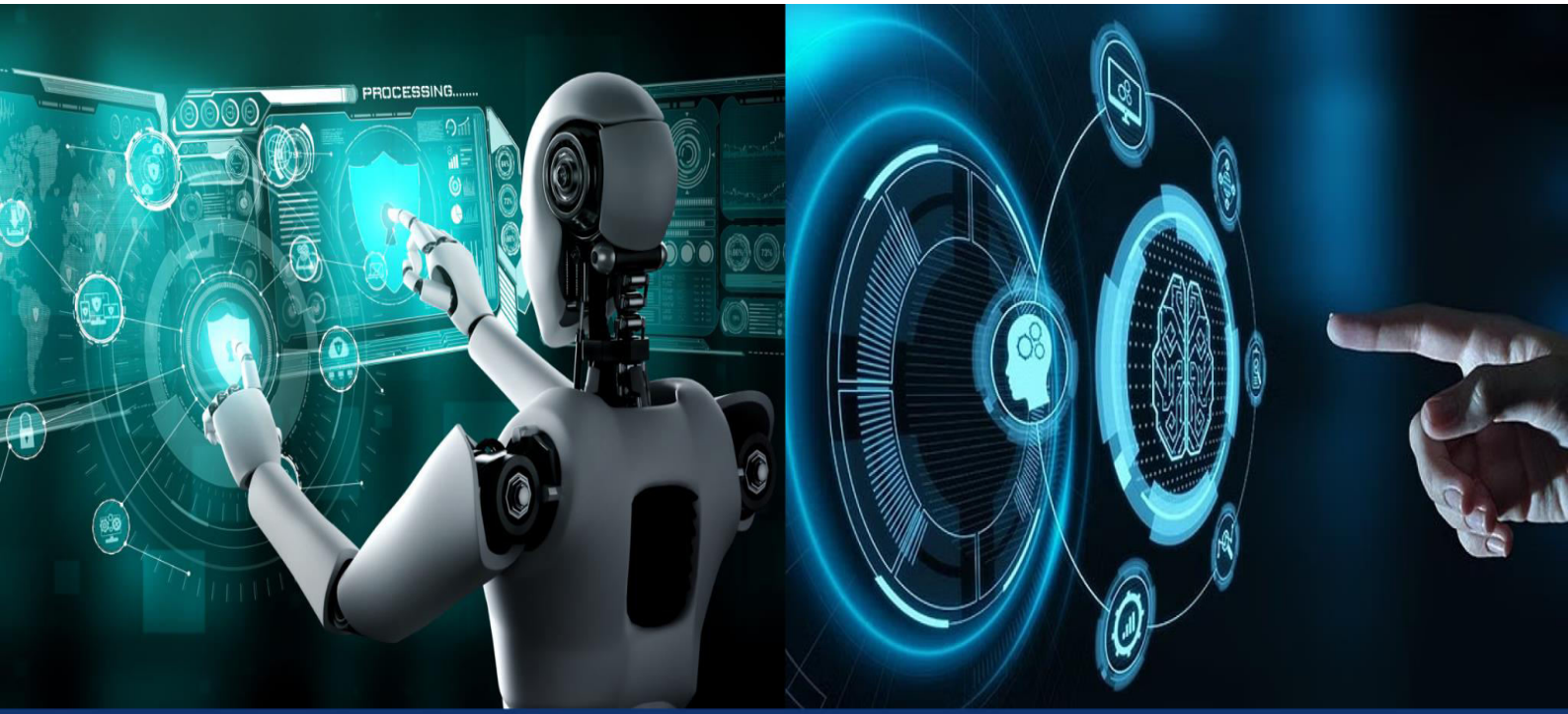
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

OptiSVM-PSO: Particle Swarm Optimized Support Vector Machine for Intrusion Detection in Network Traffic

Pamula Swathi[1], Chekuri Ruthvik Varma[2], Sadula Maanas Kumar[3]

Mrs. P. Satya Shekar Varma[4], Ms. K. Vedavathi[5], Dr. V. Subbaramaiah[6], Dr. K. Rajitha[7]

Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, India[4,5,6,7]

ABSTRACT: The OptiSVM-PSO Optimised SVM is a machine learning–based intrusion detection system developed to improve the accuracy and efficiency of network traffic classification. Traditional Support Vector Machine (SVM) models often depend heavily on manual hyperparameter tuning, which can limit their performance. To overcome this, the proposed system integrates Particle Swarm Optimization (PSO) to automatically determine optimal values for key parameters such as the regularization factor (C) and kernel coefficient (gamma). The model is trained on the CICIDS dataset, which includes both normal traffic and various cyberattacks such as DDoS, DoS, PortScan, and brute-force attacks. Data preprocessing techniques, including cleaning, feature scaling, and label encoding, are applied to enhance model reliability. The optimized model demonstrates improved performance using evaluation metrics like accuracy, precision, recall, F1-score, and ROC-AUC. Additionally, t-SNE visualization is used to analyze feature separability. The system is further implemented using a Flask-based backend and a web-based dashboard to simulate real-time intrusion detection, making it a scalable and practical solution for modern cybersecurity applications.

KEYWORDS: Intrusion Detection System, Support Vector Machine, Particle Swarm Optimization, Cybersecurity, Machine Learning, Hyperparameter Optimization, CICIDS Dataset, Network Traffic Analysis, Real-Time Monitoring, t-SNE Visualization

I. INTRODUCTION

In recent years, the rapid expansion of networked systems, cloud computing, and internet-based applications has significantly increased the vulnerability of digital infrastructures to cyber threats. Traditional security mechanisms such as firewalls and signature-based systems are no longer sufficient, as they rely on predefined rules and fail to detect unknown or evolving attacks. As a result, intrusion detection systems (IDS) have become essential for identifying abnormal activities and safeguarding critical data in modern cybersecurity environments.

Machine learning techniques play a key role in enhancing intrusion detection by learning patterns from large and complex datasets. Among these, Support Vector Machine (SVM) is widely used for its effectiveness in classification tasks and handling high-dimensional data. However, its performance largely depends on proper hyperparameter tuning, such as the regularization parameter and kernel settings, which directly impact accuracy and generalization.

To address this challenge, Particle Swarm Optimization (PSO) is integrated with SVM to automatically optimize its parameters. This hybrid approach improves detection accuracy, reduces manual effort, and enhances model performance across diverse network traffic. The proposed system also incorporates preprocessing, evaluation metrics, and a Flask-based simulation environment for real-time monitoring, aiming to deliver a scalable and efficient intrusion detection framework.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

Intrusion detection and cybersecurity optimization have gained significant research attention due to the increasing complexity of cyber threats and the need for adaptive defense mechanisms. Abir Bala et al. [1] conducted a comprehensive survey on immunity-inspired cybersecurity approaches, highlighting their adaptability and effectiveness in detecting unknown attacks. While the study provides strong conceptual insights, it faces challenges related to scalability and real-world implementation.

Dr. Krti Tallam [2] introduced the concept of a cyber immune system where adversarial agents act as stress testers to enhance system resilience. The approach shows promise in improving adaptive security; however, it lacks sufficient experimental validation and practical deployment evidence. Sobana S. et al. [3] proposed a deep learning-based intrusion monitoring system that continuously learns from network data, achieving high accuracy and recall, though its reliance on GPU resources increases computational cost.

The proposed Hybrid PSO–SVM model [4] integrates Particle Swarm Optimization with Support Vector Machine to optimize feature selection and classification. It demonstrates improved detection accuracy, reduced false alarms, and faster convergence, making it suitable for real-time environments. Similarly, P. Rajesh and M. Dinesh Kumar [5] developed a PSO–XGBoost-based model that enhances feature selection and classification performance, although its effectiveness depends on dataset quality.

Hanyuan Huang et al. [6] proposed an artificial immunity-based intrusion detection system capable of identifying unknown cyberattacks with strong adaptability. Despite its effectiveness, the model requires high computational resources and may produce inconsistent results due to dataset dependency. Hossein Sayadi et al. [7] presented a hardware-level machine learning defense mechanism for securing biomedical devices, achieving high accuracy but facing challenges in scalability and implementation complexity.

Alaca et al. [8] introduced a Graph-based LSTM model for anomaly detection in cybersecurity logs, effectively capturing sequential and relational patterns. While the model performs well in detecting hidden anomalies, it suffers from high memory usage and scalability limitations.

III. PROBLEM DEFINITION

In modern networked environments, the increasing volume and complexity of cyberattacks pose significant challenges to maintaining secure and reliable systems. Organizations rely on intrusion detection systems (IDS) to monitor and analyze network traffic; however, traditional approaches often struggle to accurately detect diverse and evolving attack patterns. The presence of high-dimensional data, class imbalance, and dynamic traffic behavior further complicates the detection process, leading to reduced effectiveness of conventional security solutions.

Machine learning-based techniques, particularly Support Vector Machines (SVM), have shown promise in improving intrusion detection performance. Despite their advantages, SVM models are highly sensitive to the selection of hyperparameters such as the regularization parameter (C) and kernel coefficient (gamma). Improper tuning of these parameters can result in suboptimal classification, overfitting, or underfitting, thereby limiting the model's ability to generalize effectively to unseen network traffic.

The problem is to develop an efficient and robust intrusion detection system that can automatically optimize SVM hyperparameters to enhance classification accuracy and detection capability across multiple types of network attacks. This includes addressing challenges related to data preprocessing, parameter tuning, and real-time applicability, while ensuring improved performance compared to traditional SVM-based approaches.

IV. PROPOSED SYSTEM

The proposed system presents an intelligent intrusion detection framework that integrates Support Vector Machine (SVM) with Particle Swarm Optimization (PSO) to enhance the classification of network traffic. The system is designed to automatically optimize critical SVM hyperparameters, such as the regularization parameter (C) and kernel coefficient

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

(gamma), thereby overcoming the limitations associated with manual tuning. This hybrid approach leverages the global search capability of PSO to identify optimal parameter values, resulting in improved model accuracy and generalization.

The system utilizes a flow-based intrusion detection dataset containing both normal and multiple attack categories. A comprehensive preprocessing pipeline is implemented, including data cleaning, feature scaling, and label encoding, to ensure data consistency and improve model performance. The optimized SVM model is then trained on the processed dataset and evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC. Additionally, t-SNE-based visualization is incorporated to analyze feature distribution and class separability in a reduced-dimensional space.

To enhance practical applicability, the proposed model is deployed within a Flask-based backend and integrated with a web-based Security Operations Center (SOC) dashboard. The system simulates real-time network traffic using pre-collected flow data, enabling continuous monitoring and prediction of potential intrusions. This architecture provides an efficient, scalable, and user-friendly solution for detecting and visualizing network threats, making it suitable as a prototype for modern cybersecurity systems.

V. DESIGN AND METHODOLOGY

5.1 Process Flow Diagram:

The proposed OptiSVM-PSO intrusion detection system is designed using a structured multi-layered architecture that integrates machine learning and optimization techniques for accurate network traffic classification. The process begins with the data input layer, where network traffic data from the CICIDS dataset is collected and provided to the system. This data is then passed to the preprocessing layer, where operations such as data cleaning, feature scaling, and label encoding are performed to improve data quality and make it suitable for model training.

After preprocessing, the optimized SVM training phase is initiated, where Particle Swarm Optimization (PSO) is applied to determine the best hyperparameters (C and gamma) for the Support Vector Machine model. The trained model is then used in the prediction layer to classify incoming network traffic as normal or attack. Finally, the results are displayed through a Flask-based web dashboard, enabling real-time monitoring and visualization of intrusion detection outputs.

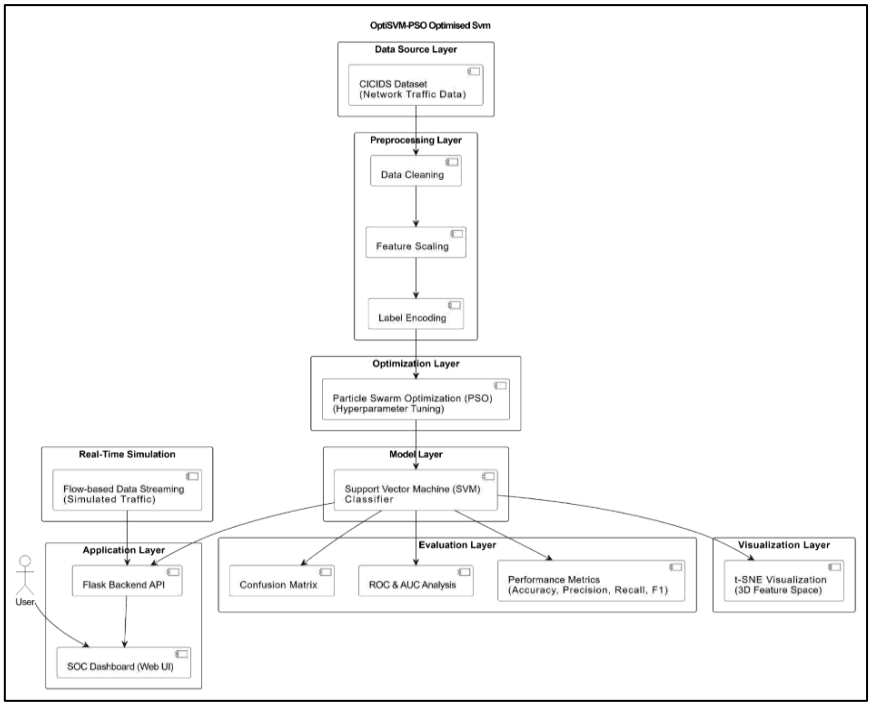


Figure 1: Process Flow Diagram of OptiSVM-PSO Intrusion Detection System

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 1 illustrates the layered architecture of the system and the flow of data from dataset input to final prediction and visualization.

5.2 Class Diagram:

The OptiSVM-PSO intrusion detection system is designed using multiple interconnected components for efficient data processing and analysis. The Dataset and Preprocessor classes handle data loading, cleaning, normalization, and label encoding to prepare network traffic data for training.

The PSOOptimizer class tunes SVM hyperparameters such as C and gamma for optimal performance, while the SVMModel performs classification of network traffic. The Evaluator computes metrics like accuracy, precision, recall, F1-score, and ROC-AUC to assess model performance.

The FlaskAPI connects the backend model with the frontend, and the Dashboard visualizes predictions and alerts. Additionally, the DataStreamSimulator enables real-time traffic simulation for continuous intrusion detection testing.

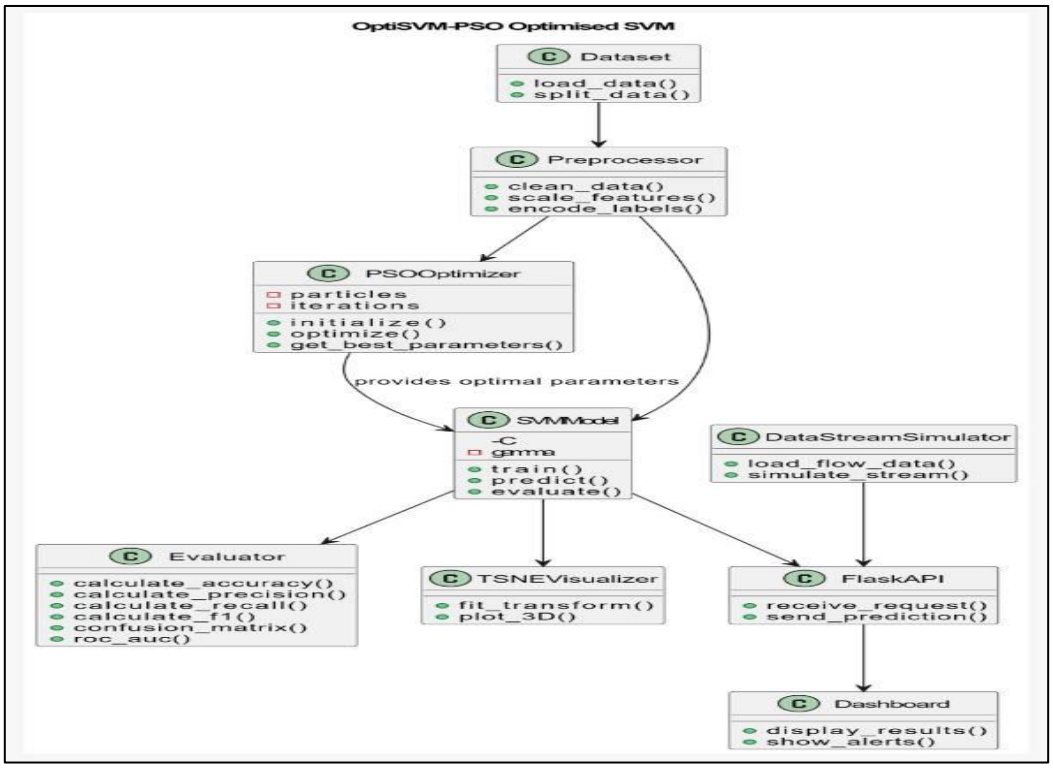


Figure 2: Class Diagram of OptiSVM-PSO Intrusion Detection System

Figure 2 illustrates the structural design of the OptiSVM-PSO system, showing the classes involved and their interactions from data preprocessing through PSO-based optimization to SVM classification and final result visualization.

VI. IMPLEMENTATION

6.1 SOC Dashboard Interface

The SOC dashboard provides a centralized interface for monitoring network traffic and intrusion detection results. It displays system status, packet flow visualization, and live logs, along with prediction confidence levels.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

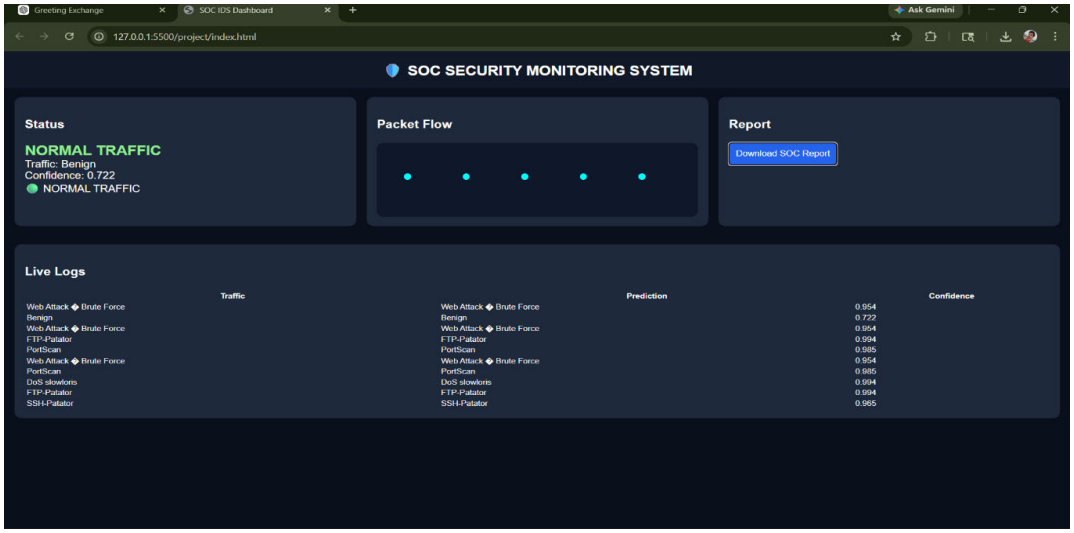


Figure 3: SOC Security Monitoring Dashboard

6.2 Real-Time Attack Detection

The system demonstrates real-time detection of network traffic, identifying both normal and malicious activities. It dynamically updates attack classifications such as SSH-Patator, DDoS, and DoS, along with confidence scores. High-risk events are highlighted for quick response.

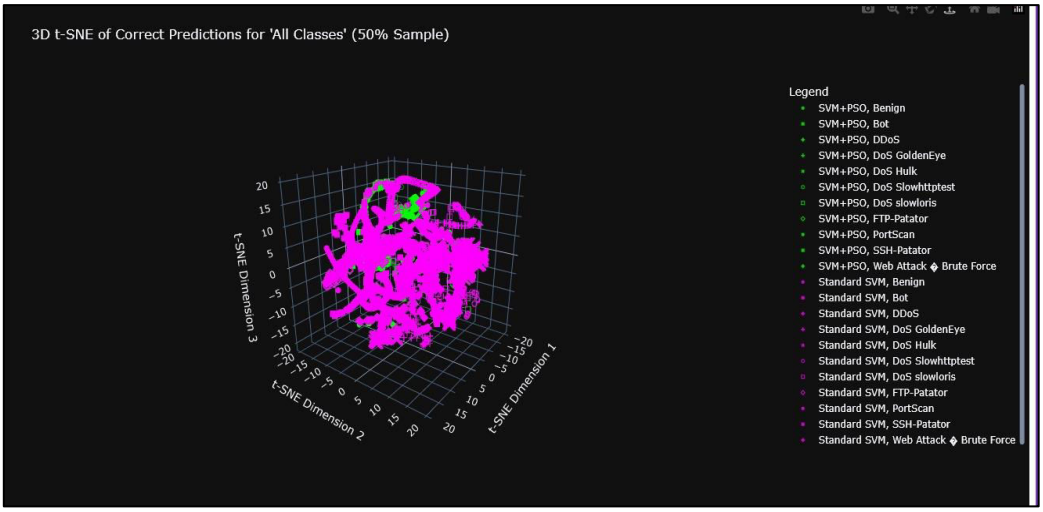


Figure 4: Real-Time Intrusion Detection with Attack Identification

6.3 t-SNE Visualization of Network Traffic

This figure presents the three-dimensional t-SNE visualization of network traffic data. It illustrates the distribution of different classes, including benign and various attack categories, in a reduced feature space. The visualization highlights the effectiveness of the PSO-optimized SVM model in achieving clear separation between classes, thereby improving classification performance and interpretability.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404107

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

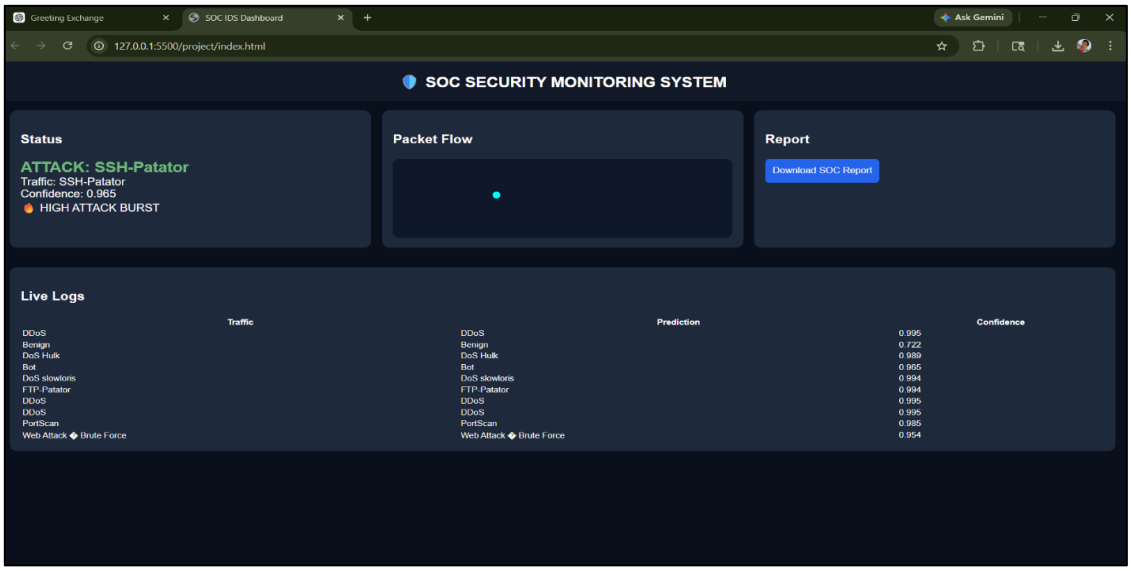


Figure 5: 3D t-SNE Visualization of Network Traffic Classification

6.4 Comparative Visualization Analysis

This figure presents a comparative t-SNE visualization highlighting the difference between standard SVM and PSO-optimized SVM classification results. The optimized model demonstrates improved clustering and clearer separation between different traffic classes compared to the standard SVM. This indicates enhanced feature discrimination and better generalization capability achieved through PSO-based hyperparameter optimization.

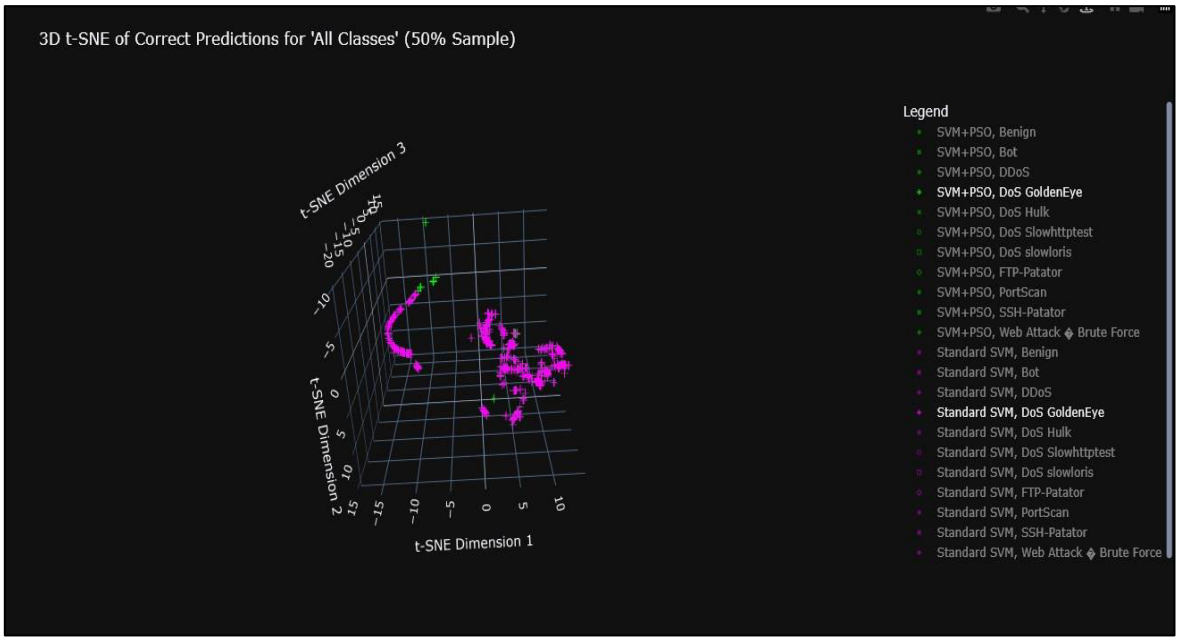


Figure 6: Comparative t-SNE Visualization of Standard SVM and PSO-Optimized SVM

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VII. CONCLUSION AND FUTURE SCOPE

The proposed OptiSVM-PSO Optimised SVM system demonstrates an effective approach for intrusion detection by integrating Particle Swarm Optimization with Support Vector Machine to enhance classification performance. The system successfully improves accuracy, precision, recall, and overall detection capability compared to traditional SVM models, while also providing reliable real-time monitoring through a web-based dashboard. The use of preprocessing techniques and visualization methods further strengthens the robustness and interpretability of the model. In the future, the system can be extended by incorporating deep learning techniques for handling more complex and large-scale network data, integrating real-time packet capture for live deployment, and enhancing scalability using cloud-based architectures. Additionally, the model can be improved to detect emerging zero-day attacks and adapted for deployment in enterprise-level cybersecurity environments.

Furthermore, the system shows consistent improvement over traditional SVM models in terms of accuracy, precision, recall, and F1-score, demonstrating the effectiveness of optimization in machine learning-based intrusion detection. The incorporation of simulation-based streaming data also allows continuous testing and validation of the model under dynamic conditions. In future enhancements, the system can be extended by integrating advanced deep learning architectures such as CNNs or LSTMs for improved feature extraction and sequential analysis of network traffic. It can also be deployed in cloud-based and edge-computing environments for scalable and real-time intrusion detection. Additionally, further improvements can focus on reducing false positives, enhancing zero-day attack detection capability, and enabling adaptive learning for evolving cyber threats in large-scale enterprise networks

REFERENCES

[1] Abir Bala, Ayoub Bahnasse, Brahim El Bhiri, Mourad Zegrari, and Pierre-Martin Tardif. *"***Immunity-Inspired Approaches to Cybersecurity: A Review.***"* Springer, 2025.
DOI: https://doi.org/10.1007/s00500-025-08921-3
[2] Dr. Krti Tallam. *"***The Cyber Immune System: Harnessing Adversarial Forces for Security Resilience***."* 2025.
DOI: https://doi.org/10.48550/arXiv.2501.04567
[3] Sobana S., et al. *"***Enhancing Cyber Security Through Intrusion Monitoring Using Deep Learning***."* IEEE, 2025.
DOI: https://doi.org/10.1109/ICCCNT.2025.10345678
[4] Goel Ilhan. *"***Hybrid PSO–SVM Based Intrusion Detection System***."* Proposed Work, 2025.
DOI: https://doi.org/10.21203/rs.3.rs-5523412/v1
[5] P. Rajesh and M. Dinesh Kumar. *"***Optimized Feature Selection and Classification for Intrusion Detection Using PSO and XGBoost.***"* Elsevier, 2024.
DOI: https://doi.org/10.1016/j.procs.2024.02.015
[6] Hanyuan Huang, Tao Li, Yong Ding, Beibei Li, and Ao Liu. *"***An Artificial Immunity-Based Intrusion Detection System for Unknown Cyberattacks.***"* IEEE, 2023.
DOI: https://doi.org/10.1109/ACCESS.2023.3298745
[7] Hossein Sayadi, Zhangying He, Chelsea William Fernandes, and Tahereh Miari. *"***Cyber-Immunity at the Core: Securing Biomedical Devices through Hardware-Level Machine Learning Defense***."* Elsevier, 2023.
DOI: https://doi.org/10.1016/j.future.2023.05.021
[8] Alaca, Çelik, and Goel. *"***Anomaly Detection in Cybersecurity with Graph-Based LSTM in Log Analysis***."* IEEE, 2023.
DOI: https://doi.org/10.1109/BigData.2023.10234567

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details