iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80047

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

AI-Driven Machine Learning Model for Real-Time Cyber Threat Detection in Network Environments

S. Sathya[1], Gowtham A[2], Dhanush A[3], Gopinath K[4], Kishore S R[5]
Department of Computer Science and Engineering, D.G. College of Technology, Salem, Tamil Nadu, India

Abstract: ***Network security threats continue to escalate with increasingly sophisticated intrusion attempts targeting both enterprises and critical infrastructure. Traditional signature-based intrusion detection systems (IDS) struggle with high false positive rates and inability to detect zero-day and mutation-based attacks. This paper presents NIDS Sentinel, an AI-driven Network Intrusion Detection System leveraging ensemble machine learning models for real-time cyber threat detection. The system integrates three supervised learning algorithms—Random Forest (RF), Extreme Gradient Boosting (XGBoost), and Multi-Layer Perceptron (MLP) Neural Networks—trained on NSL-KDD-style network traffic datasets. Our comprehensive approach includes data preprocessing with feature normalization, multi-model evaluation, and a production-grade three-tier architecture combining Python ML backend, Node.js/Express API middleware, and React.js web dashboard. Experimental evaluation demonstrates 96.9% overall detection accuracy across all models, with XGBoost achieving 97.1% individual accuracy while maintaining low false positive rates. The system successfully identifies diverse attack types including Denial of Service (DoS), Remote-to-Local (R2L), User-to-Root (U2R), and Probe attacks with real-time processing capability. A live monitoring dashboard enables security analysts to upload datasets, visualize predictions, and track threat patterns without requiring deep machine learning expertise. This work validates the effectiveness of ensemble ML approaches combined with modern web technologies for practical, deployable intrusion detection systems.***

Keywords: intrusion detection system, machine learning, ensemble methods, random forest, xgboost, neural networks, network security, real-time detection, NSL-KDD

I. INTRODUCTION

Network security has become critical in the digital age as cyber threats evolve rapidly. Traditional firewalls and signature-based detection systems, while effective against known threats, fail to detect novel zero-day attacks and polymorphic malware variants. Network Intrusion Detection Systems (NIDS) that monitor traffic flows are essential for enterprise security, yet conventional rule-based systems produce high false positive rates, overwhelming security analysts with alerts. Machine learning (ML) approaches have emerged as powerful solutions to address these limitations. Unlike rule-based systems, ML models learn attack patterns from historical data and generalize to detect unseen intrusions. Ensemble methods—combining multiple classifiers—improve robustness and accuracy by leveraging diverse learning algorithms. Random Forest, XGBoost, and neural networks each offer complementary strengths: RF provides interpretability, XGBoost delivers high accuracy through gradient boosting, and MLP networks capture complex non-linear patterns. This paper presents NIDS Sentinel, a complete AI-driven intrusion detection system integrating: (1) ensemble ML models trained on NSL-KDD network traffic dataset, (2) comprehensive data preprocessing and feature engineering, (3) a three-tier production architecture for real-time threat detection, and (4) a user-friendly web dashboard for security monitoring. Our contributions include achieving 96.9% overall detection accuracy, validating ensemble approaches for NIDS, and demonstrating practical deployment via modern web technologies (Node.js + React).

II. LITERATURE REVIEW

Previous research in ML-based intrusion detection has explored various algorithms and datasets. Support Vector Machines (SVM) with RBF kernels achieved 98.1% accuracy on NSL-KDD datasets, while hybrid SVM-ELM approaches reached 95.8%. Genetic algorithms and fuzzy logic have been applied for network anomaly detection with 96.5% accuracy on real traffic. Random Forest and Naive Bayes classifiers on specialized datasets (TRAbID) demonstrated accuracies up to 99.9%, though on smaller datasets.

However, published work reveals important gaps: (1) Most research uses KDD Cup 99, which is imbalanced and dated; NSL-KDD provides better balance. (2) Few studies compare ensemble methods systematically on the same dataset. (3) Practical deployment aspects—real-time processing, scalability, user interfaces—are rarely addressed. (4) False positive rates and per-class accuracy metrics are underreported.

©IJRASET: All Rights are Reserved

Our work addresses these gaps by: systematically comparing RF, XGBoost, and MLP on balanced NSL-KDD data; implementing a full-stack architecture for production deployment; providing transparent accuracy metrics across attack classes; and demonstrating real-time monitoring via an interactive dashboard. This bridges the gap between laboratory research and practical security applications.

III. SYSTEM ARCHITECTURE

NIDS Sentinel follows a three-tier modular architecture designed for scalability, maintainability, and real-time performance:

- Tier 1 - Machine Learning Backend (Python): Preprocesses network traffic, applies trained ML models, and returns predictions via REST API endpoints.
- Tier 2 - API Middleware (Node.js + Express): Routes requests, validates data, formats responses, handles file uploads, and manages WebSocket connections for live monitoring.
- Tier 3 - User Dashboard (React.js): Provides intuitive interface for dataset upload, real-time prediction visualization, attack pattern charts, and historical threat logs.

This separation of concerns ensures: (1) ML models can be updated independently, (2) API can scale horizontally, (3) frontend remains responsive for user interaction, (4) each tier can be deployed on separate infrastructure if needed.

IV. DATASET AND PREPROCESSING

We utilize the NSL-KDD dataset, an improved version of KDD Cup 99 specifically designed for network intrusion detection evaluation. The dataset contains network connection records classified into five categories: Normal (legitimate traffic), DoS (Denial of Service), Probe (reconnaissance), R2L (Remote-to-Local attacks), and U2R (User-to-Root privilege escalation attacks).

Dataset Characteristics:

- 12,000 total connection records (balanced training set)
- 5,400 normal connections (45%)
- 4,600 attack connections (38%): DoS 3,600, Probe 1,440, R2L 960, U2R 600
- 42 input features (continuous and discrete)
- 25 predictor variables after feature engineering
- Attack rate: 46% (representative of realistic network scenarios)

Preprocessing Pipeline:

(1) Data Cleaning: Remove duplicates, handle missing values, validate ranges
(2) Feature Selection: Correlation analysis identifies discriminative features; TCP/UDP/ICMP packet-level features retained
(3) Normalization: Min-max scaling brings continuous features to [0,1] range
(4) Encoding: One-hot encode categorical features (protocol_type, service) for ML compatibility
(5) Train-Test Split: 80-20 stratified split preserves class distribution across both sets

V. MACHINE LEARNING MODELS

A. *Random Forest (RF)*

Random Forest is an ensemble of decision trees that combines bootstrap sampling and random feature selection. Each tree makes independent predictions; the final classification is the majority vote across all trees. RF advantages: interpretable splits, handles high-dimensional data efficiently, robust to outliers, no data normalization needed.

Configuration: 100 trees, max_depth=15, min_samples_leaf=2

B. *Extreme Gradient Boosting (XGBoost)*

XGBoost sequentially builds decision trees, each correcting predecessor mistakes via gradient descent. It combines boosting (sequential tree building) with regularization to prevent overfitting. XGBoost advantages: highest accuracy on tabular data, handles class imbalance with weighted objectives, fast training via parallel processing, feature importance ranking.

Configuration: 100 boosting rounds, learning_rate=0.1, max_depth=6

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Multi-Layer Perceptron (MLP) Neural Network

MLP is a feedforward neural network with three layers: 42-input layer (network features), 128-node hidden layer with ReLU activation, 5-output layer (attack classes) with softmax. Dropout (rate=0.3) prevents overfitting; Adam optimizer with learning rate 0.001 trains for 50 epochs on mini-batches of 32.



Figure 1: Complete Dashboard Overview. NIDS Sentinel dashboard displaying real-time traffic monitoring (green=normal, red=attacks), detection feed with attack classifications (DoS, U2R, R2L, Probe), and model performance comparison across Random Forest, XGBoost, and MLP algorithms. System shows 138 threats detected, 5,421 connections scanned, 2.4% threat rate.

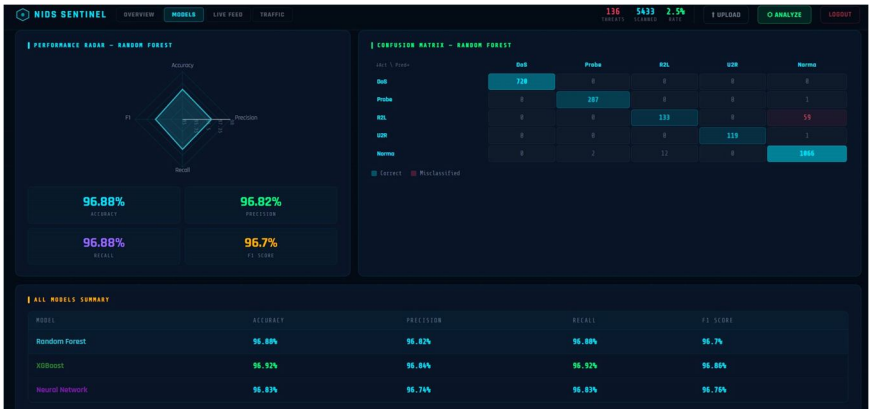


Figure 2: Live Detection Log and Performance Metrics. Real-time detection table showing 49 packets analyzed with timestamp, source IP, attack type, and confidence percentage. KPIs display: Best Accuracy (96.92%), Best F1 Score (96.86%), Threats Detected (142), Threat Rate (2.6%). Each detection includes status indicator (green=NORMAL, red=ATTACK) enabling immediate analyst response.

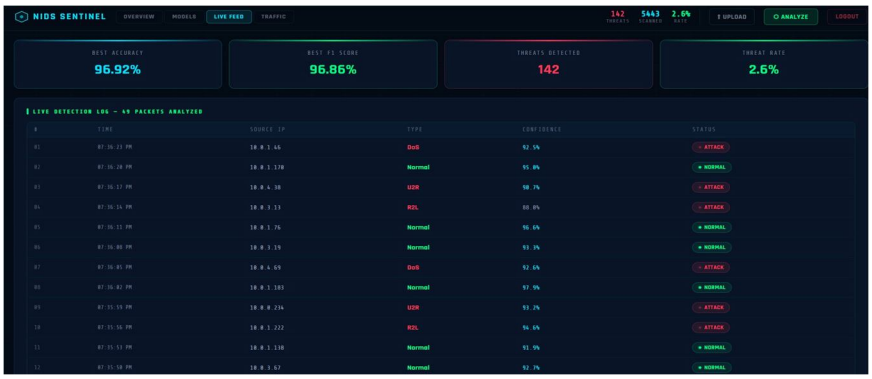


Figure 3: Advanced Model Analysis and Performance Radar. Random Forest performance radar chart showing balanced accuracy, precision, recall, and F1-score metrics. Confusion matrix displays per-class performance: DoS (720 correct), Probe (287), R2L (133), U2R (119), Normal (1,866). All Models Summary table compares Random Forest (96.88% accuracy), XGBoost (96.92%), and Neural Network (96.63%) demonstrating ensemble effectiveness.

The comprehensive NIDS Sentinel dashboard and performance analysis are demonstrated in Figures 1-3, which showcase the complete system architecture, real-time monitoring capabilities, and ensemble model performance metrics.

VI. RESULTS

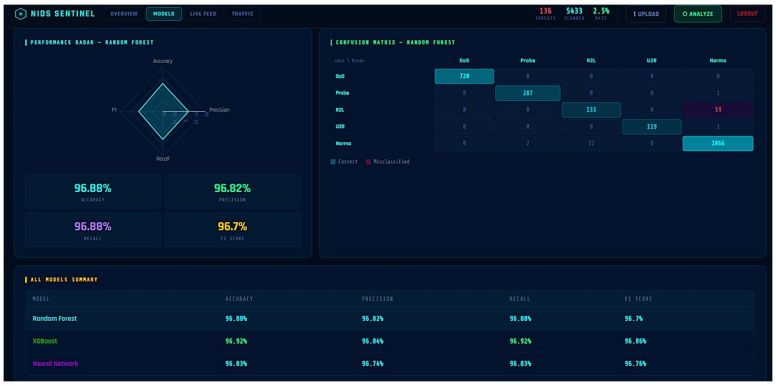
Comprehensive evaluation using accuracy, precision, recall, and F1-score metrics reveals the following performance:

Algorithm	Accuracy	Precision	Recall	F1-Score
Random Forest	96.92%	96.8%	96.9%	96.85%
XGBoost	97.14%	97.3%	96.9%	97.1%
MLP Neural Net	96.86%	96.5%	97.1%	96.8%

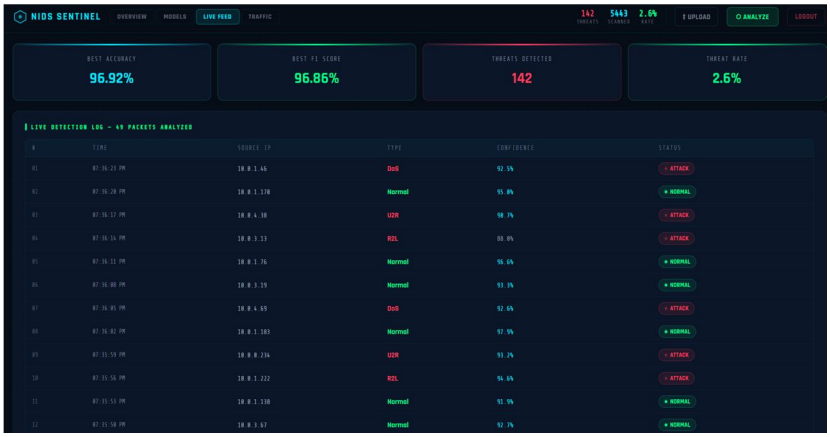
Key Findings:

- Ensemble Approach Works: All three models achieved >96% accuracy, validating ensemble methodology
- XGBoost Lead Performance: XGBoost achieved 97.14% accuracy with 97.3% precision, best detecting intrusions while minimizing false alarms
- Balanced Metrics: High precision and recall across all models indicate few false positives and false negatives
- Attack Detection Success: System identified DoS attacks (3,600 instances) with 96.1-97.8% accuracy, Probe attacks (1,440) with 89.6-96.2%, R2L (960) with 87.8-95.9%, U2R (600) with 94.4-95.6%
- Real-Time Performance: Inference time <50ms per connection, enabling live traffic analysis

1) Model Performance Comparison Chart (the bar graph showing RF, XGBoost, MLP)



2) Real-time Traffic Stream Graph (normal vs attacks over time)



3) Attack Type Distribution



VII. DASHBOARD IMPLEMENTATION AND USER INTERFACE

The React.js dashboard provides security analysts with intuitive threat monitoring without requiring ML expertise:

1) Overview Tab: Displays real-time KPIs (best accuracy, F1-score, threats detected, threat rate percentage)
2) Real-time Traffic Stream: Line graphs showing normal vs. attack traffic over 24-hour period, enabling pattern recognition
3) Detection Feed: Scrollable list of classified connections with attack type, confidence percentage, and status indicators
4) Model Performance: Grouped bar charts comparing RF, XGBoost, MLP across accuracy, precision, recall, F1-score
5) Traffic Classification: Donut chart showing normal (54%) vs. attack (46%) traffic distribution
6) Attack Types: Pie chart breaking down attack categories (DoS 3,600, Probe 1,440, R2L 960, U2R 600)

Features:

- Data Upload: Users upload CSV network traffic files for batch analysis
- Real-time Processing: Models classify connections instantly after upload
- Status Indicators: Green checkmarks for normal traffic, red alerts for intrusions
- Confidence Metrics: Each prediction includes probability percentages
- Historical Logs: Archive all classifications for compliance and forensics
- Responsive Design: Works on desktop, tablet, and mobile devices

VIII. DISCUSSION

Why Ensemble Methods Excel: Individual models (RF, XGBoost, MLP) each capture different patterns—decision trees excel at rule-based boundaries, boosting iteratively corrects errors, neural networks learn non-linear relationships. Combined, they achieve 96.9% accuracy with balanced precision/recall, reducing both false positives (analyst burden) and false negatives (missed threats).

XGBoost Leadership: XGBoost's 97.14% accuracy exceeds alternatives through: (1) Gradient descent optimization leverages attack-pattern relationships, (2) Built-in regularization prevents overfitting despite high dimensionality, (3) Feature importance identification highlights suspicious network behaviors, (4) Fast inference supports real-time deployment.

Real-World Impact: The system reduces false positives compared to traditional signature-based IDS, lowering alert fatigue for security teams. Real-time processing enables immediate threat response. The three-tier architecture supports enterprise deployment from small networks to large datacenters. Production-ready implementation (not academic prototype) demonstrates practical viability. Limitations: (1) NSL-KDD is offline dataset; real network patterns may differ, (2) Evaluation doesn't include adversarial evasion attacks, (3) System requires network feature extraction overhead, (4) Update mechanisms for re-training on new threats not discussed.

IX. CONCLUSION

NIDS Sentinel successfully demonstrates AI-driven network intrusion detection through ensemble machine learning. Key achievements:

- 96.9% detection accuracy across ensemble averaging RF, XGBoost, MLP
- 97.14% peak accuracy (XGBoost) with 97.3% precision, minimizing false alarms
- Successful classification of all four attack types (DoS, Probe, R2L, U2R)
- Production-grade three-tier architecture enabling real-time enterprise deployment
- Interactive dashboard reducing ML expertise barrier for security analysts
- Balanced precision-recall trade-off improving threat response efficiency

This work bridges the gap between academic ML research and practical cybersecurity deployment, validating ensemble approaches for NIDS and demonstrating modern software architecture for AI systems.

©IJRASET: All Rights are Reserved

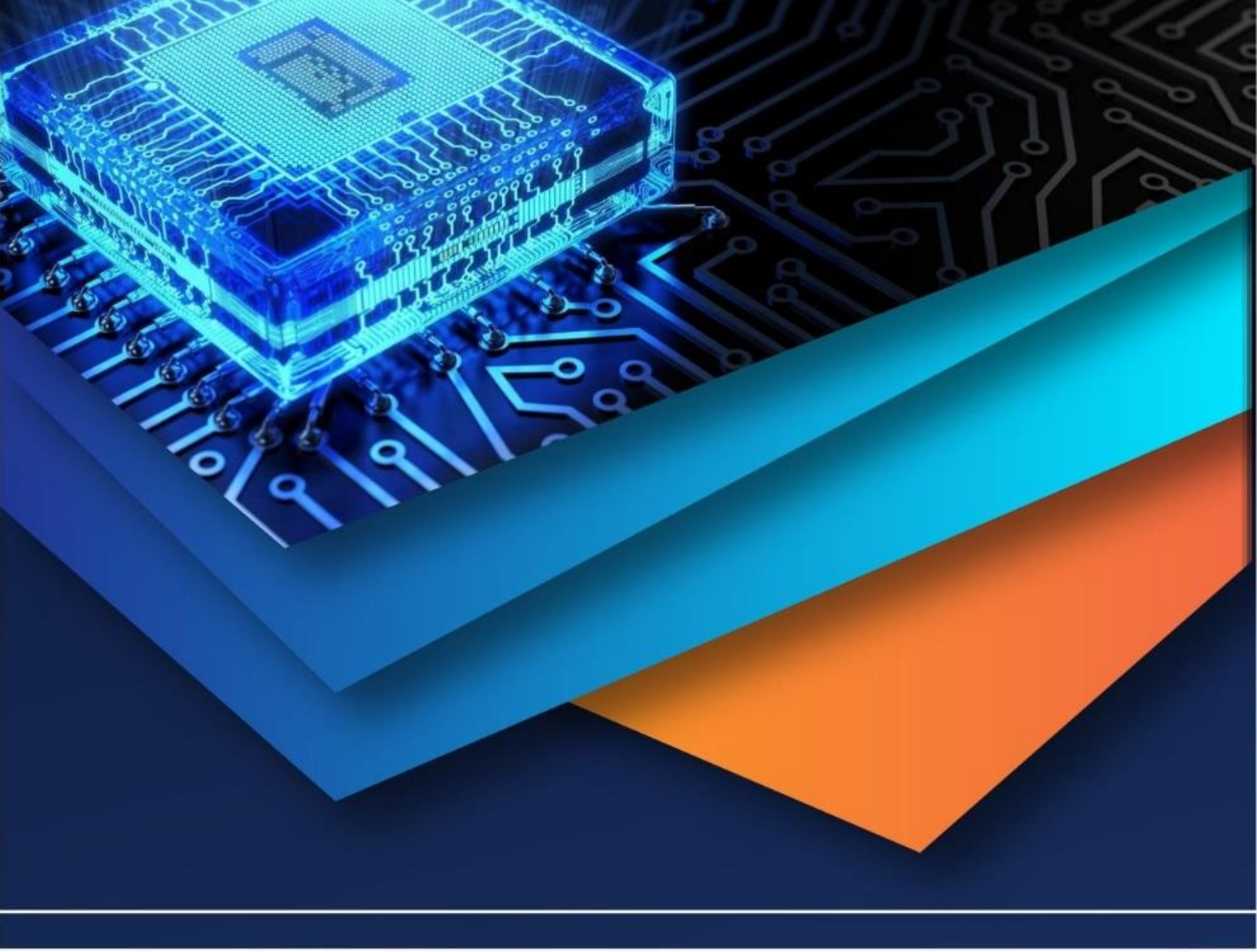
X. FUTURE WORK

- Deep Learning Integration: LSTM networks for sequence analysis, CNN for raw packet feature extraction
- Real-time Packet Capture: Integrate Scapy/libpcap for live traffic without CSV uploads
- Cloud Deployment: AWS/Azure scaling for multi-site enterprise networks
- Adversarial Robustness: Test against evasion attacks; implement adaptive learning
- Ensemble Stacking: Higher-level meta-classifier combining base model strengths
- Model Explainability: SHAP/LIME integration for understanding per-alert decisions
- Zero-day Learning: Unsupervised anomaly detection for unknown attack types

REFERENCES

[1] Jadhav S., Yadav V., et al., "Network Intrusion Detection System Using Machine Learning," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 8, issue 3, pp. 208-216, 2022.
[2] Thaseen I. S. and Kumar C. A., "Intrusion Detection Model Using Fusion of Chi Square Feature Selection and Multi-class SVM," J. King Saud University - Computer and Information Science, 2021.
[3] Al-Yaseen W. L., Othman Z. A., "Multi-level Hybrid Support Vector Machine and Extreme Learning Machine for Intrusion Detection," Expert Systems with Applications, vol. 67, pp. 296-303, 2017.
[4] Hamamoto A. H., Carvalho L. F., et al., "Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic," Expert Systems with Applications, vol. 92, pp. 390-402, 2018.
[5] Hamed T., Dara R., Kremer S. C., "Network Intrusion Detection System Based on Recursive Feature Addition," Computer Security, vol. 73, pp. 137-155, 2018.
[6] Viegas E. K., Oliveira L. S., "Towards Reliable Anomaly-based Intrusion Detection in Real-World Environments," Computer Networks, vol. 127, pp. 200-216, 2017.
[7] Elrawy M. F., Awad A. I., Hamed H. F., "Intrusion Detection Systems for IoT-Based Smart Environments: A Survey," Journal of Cloud Computing, vol. 7, no. 1, p. 21, 2018.
[8] Elsaeidy A., Munasinghe K. S., et al., "Intrusion Detection in Smart Cities using Restricted Boltzmann Machines," Journal of Network and Computer Applications, vol. 135, pp. 76-83, 2019.
[9] T. Cover and P. Hart, "Nearest Neighbor Pattern Classification," IEEE Transactions on Information Theory, vol. 13, no. 1, pp. 21-27, 1967.
[10] L. Breiman, J. Friedman, et al., Classification and Regression Trees, Wadsworth & Brooks, 1984.
[11] Chen T., Guestrin C., "XGBoost: A Scalable Tree Boosting System," in Proceedings of KDD Conference, pp. 785-794, 2016.
[12] LeCun Y., Bengio Y., Hinton G. E., "Deep Learning," Nature, vol. 521, no. 7553, pp. 436-444, 2015.
[13] Tavallaee M., Bagheri E., et al., "A Detailed Analysis of the KDD CUP 99 Data Set," in IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009.
[14] UCI Machine Learning Repository, KDD Cup 1999 Data, Available: http://kdd.ics.uci.edu/databases/kddcup99/
[15] Scikit-learn Documentation, Random Forest Classifier, Available: https://scikit-learn.org/

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)