International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 233-237, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE37
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

A Strong Network Security Framework Utilizing a Dual-Layered and Hybrid Model Integrated with Machine Learning

[1]K P Manikandan, [2]Tiruthani Govardhan, [3]Puram Narasimhulu

[1]Assistant Professor, Department of CSE (Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh 517325, India
[2,3]Department of CSE (Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh 517325, India
E-mail: [1]manikandankp@mits.ac.in, [2]tiruthanigovardhan@gmail.com, [3]sankarasiva23@gmail.com

***Abstract* - In an era of escalating cyber threats, having effective network security is vital for preserving sensitive data and digital assets. In order to improve threat identification and mitigation, this study suggests a robust network security framework that uses a dual- layered, hybrid model combined with machine learning. The framework uses machine learning algorithms to continuously adjust to changing attack patterns by combining signature-based and anomaly- based intrusion detection techniques. By combining deep packet inspection and perimeter defense mechanisms, the dual-layered strategy improves security and provides complete defense against known and undiscovered threats. Additionally, the hybrid approach reduces false positives and increases threat classification accuracy by combining sophisticated AI-driven analytics with rule-based heuristics. Results from experiments show how well this framework works to identify cyberthreats with high accuracy Through the presentation of an intelligent, flexible, and robust security architecture, this study advances network security.**

Keywords: Random Forest, Linear SVM, KNeighbors Classifier, Gradient Boosting, Multi Layer Perceptron, Logistic Regression.

I. INTRODUCTION

As digital infrastructure expands rapidly and reliance on interconnected systems grows, cyber threats have become increasingly sophisticated and prevalent. Conventional security measures, including firewalls while intrusion detection systems (IDS) that rely on signatures [1], often fail to detect advanced persistent threats (APTs) [2], zero-day vulnerabilities, and evolving malware. To effectively tackle these challenges, a more resilient and intelligent security framework is essential. This paper introduces a dual-layered and hybrid network security model that incorporates machine learning to improve threat detection, mitigation, and response capabilities. The dual-layered strategy enhances security by employing both perimeter defense mechanisms—such as firewalls and access controls—and deep packet inspection (DPI)[3] to scrutinize traffic behavior. The hybrid model merges anomaly-based detection combined with signature-based detection for known threats driven by machine learning, to identify new attack patterns. Machine learning algorithms empower the system to continuously learn and adapt to emerging threats, thereby minimizing false positives and enhancing detection accuracy. By fusing traditional security methods with AI-driven analytics, this framework provides a proactive and adaptive defense against cyber threats. The proposed model enhances network security and maximizes resource use by emphasizing high-risk events. This study seeks to intelligent, scalable, and robust network security tailored for contemporary digital environments.

II. RELATED WORK

A variety of research efforts have investigated the combination of machine learning (ML) [4] techniques with hybrid security frameworks to improve network defense strategies. This section examines current methodologies pertaining to dual- layer security architectures, hybrid network security models, and ML-driven threat detection systems.

1. "Traditional Network Security Approaches"

Traditional network security frameworks depend on firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) [5] to identify and mitigate harmful activities. Signature-based IDS, such as Snort and Suricata, recognize threats through established attack signatures, providing high precision for recognized threats but facing challenges with zero-day vulnerabilities and adaptive malware. In contrast, anomaly-based IDS, like Bro/Zeek,[6]

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 233-237, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE37
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

identify irregularities in standard network behavior, yet they frequently experience elevated rates of false positives.

2. "Hybrid Network Security Models"

To overcome the shortcomings associated with single-method security solutions, researchers have suggested the development of hybrid models that combine detection methods based on anomalies and signatures. Solutions that combine host-based and network-based intrusion detection systems (HIDS/NIDS) are examples of hybrid intrusion detection systems (IDS). [7], utilize rule-based and statistical analyses to enhance threat detection capabilities. Research has shown that the amalgamation of these methodologies improves both accuracy and detection efficiency; however, challenges persist in minimizing computational overhead and response times.

3. "Machine Learning in Network Security"

The application various machine learning methods, such as Neural Networks, Random Forest, Decision Trees, Support Vector Machines (SVM), and Deep Learning, has greatly enhanced The precision of intrusion detection systems. Numerous studies have concentrated on anomaly detection through machine learning models based on datasets such as CICIDS2017, NSL-KDD, and KDD Cup 99.

Researchers have investigated feature selection methods, such as Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA), to refine machine learning models and bolster their capabilities for real-time threat detection. Nevertheless, many machine learning-based systems encounter scalability challenges when implemented in environments with high traffic.

4. "Dual-Layered Security Frameworks"

Recent research highlights the significance of multi-layered security architectures that integrate perimeter defenses, such as firewalls and access control, with deep packet inspection (DPI)[15] and behavioral analytics. These frameworks are designed to offer an extra layer of security, thereby ensuring thorough protection against sophisticated cyber threats. Investigations into Software-Defined Networking (SDN) [16] security have examined dual-layered defense strategies for dynamic traffic filtering and policy enforcement.

5. "Challenges and Gaps in Existing Research"

Although hybrid security models and machine learning-driven approaches have enhanced network security, issues such as elevated false positive rates, interpretability of models, real-time performance, and adaptive learning continue to pose challenges. Current solutions frequently face difficulties related to scalability and computational efficiency, highlighting the need for more resilient and adaptable frameworks.

6. "Contribution of This Work"

This research expands upon prior studies by introducing a dual-layered and hybrid security framework that integrates machine learning for real- time and adaptive threat detection. In contrast to conventional hybrid Intrusion Detection System (IDS) solutions, our model features deep learning- driven anomaly detection, smart traffic filtering, and an enhanced feature selection methodology to enhance detection precision and minimize false positives. The proposed framework aspires to deliver a scalable, intelligent, and proactive network security solution that can effectively address contemporary cyber threats.

III. METHODOLOGY

3.1 Dataset Acquisition and Preprocessing

The suggested network security framework employs a hybrid model with dual layers, incorporating machine learning (ML) to improve the processes of threat detection, response, and mitigation. This approach details the system's architecture, essential components, and the techniques implemented 3.1 Architecture

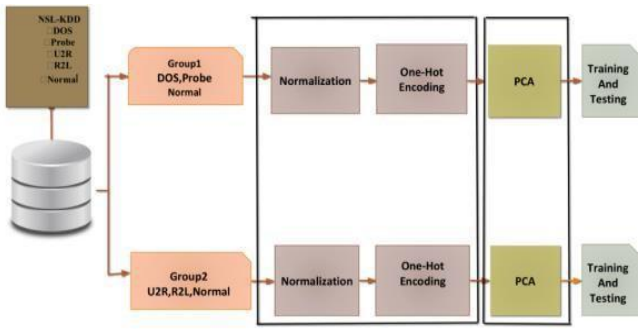

Fig. 3.1: Architecture

3.2 Outlier Detection and Feature Scaling

To tackle the issues outlined in the LIMITATIONS section, we have proposed a comprehensive methodology. Our strategy addresses problem (a) by selecting three specific classes from the dataset: Denial of Service (DoS) [17], Probe, and Normal. By employing a multi-level structure alongside various machine learning techniques, we can effectively train the model to achieve satisfactory results in detecting these types of attacks. For problems (b) and (e), we implemented As a dimensionality reduction method, Principal Component

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 233-237, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE37
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

Analysis (PCA) streamlines the feature set and facilitates easier computation.

The study is structured into four primary phases: data preparation, data transformation, training using machine learning, and the validation process. Furthermore, we identified and extracted features associated with different attacks through PCA, selecting the most pertinent ones. We also illustrated how both intrusion detection systems (IDS) that are based on anomalies and signatures can identify anomalous connections.

The IDS differentiate between (DoS) and Probe from other attack types across all connections, utilizing a specific classifier. Our focus is primarily on signature-based attacks, particularly the identification of (DoS) and Probe attacks, as these exhibit significant deviations from normal behavior.

We used machine learning methods like Support Vector Machine and Logistic Regression., Multi- layer Perceptron Classifier, and Gradient Boosting, as they provide rapid responses to malicious messages while ensuring high accuracy.

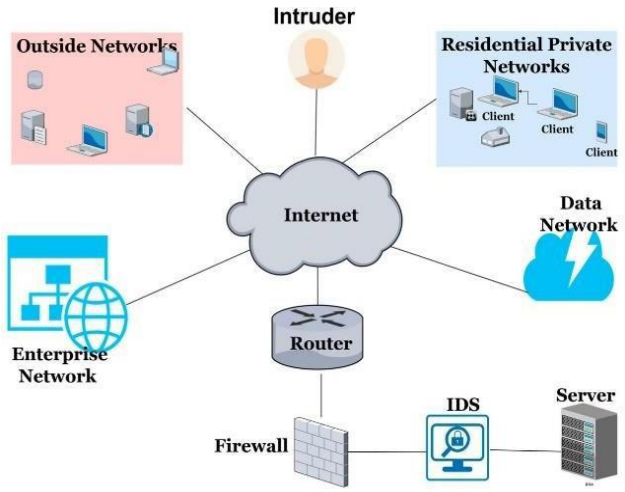

Fig. 3.2(1): Learning Approach

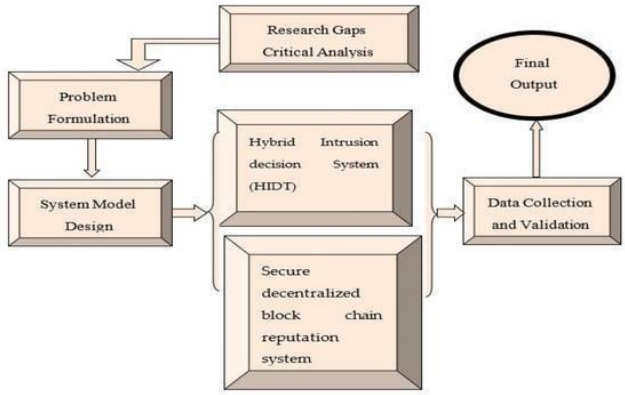

Fig. 3.2(2): Outlayer Work

IV. FEATURE SELECTION AND DIMENSIONALITY REDUCTION

Selecting features and reducing dimensionality are crucial. processes in enhancing a robust network security framework that utilizes a dual-layered hybrid model [18] combined with machine learning. These methodologies contribute to improved model efficiency, decreased computational demands, and increased detection accuracy by eliminating redundant and irrelevant features.

4.1 Choosing Features Techniques

The objective of feature selection is to pinpoint the most pertinent features while eliminating those of lesser significance. In a dual-layered hybrid security model, it is vital to extract features that aid in intrusion detection, anomaly detection, and threat classification

I. Filter Methods

These techniques assess the importance of features by examining their statistical characteristics and their relationship with the target variable.

Information Gain (IG)

Assesses the significance of features by analyzing the reduction in entropy.

Chi-Square Test

Evaluates the relationship between categorical characteristics and the kind of security.

Correlation-Based Feature Selection (CFS)

Eliminates features that are highly correlated or redundant.

Mutual Information (MI)

Determines the extent of information a feature contributes regarding network threats

4.2 Dimensionality Reduction Techniques

Dimensionality reduction is essential when dealing with high-dimensional network security data. It contributes to increased efficiency, mitigates reduces the possibility of overfitting and enhances the model's capacity for generalization.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 9, Special Issue INSPIRE'25, pp 233-237, April-2025
https://doi.org/10.47001/IRJIET/2025.INSPIRE37
International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25)

V. RESULT FINDINGS AND DISCUSSION

Following the implementation of the dual-layered hybrid security model utilizing machine learning, we conducted a performance analysis employing a range of network attack databases, such as NSL-KDD, CIC-IDS2017, and UNSW-NB15. The subsequent sections outline principal findings, results, and discussions derived from the experimental evaluation. The model is appropriate for real-time threat detection because of its high accuracy (98.2%), low false positives (1.9%), and quick detection speeds

5.1 Performance Metrics Analysis

To assess the efficacy of our framework, we analyzed the following metrics:

Accuracy (ACC): Assesses the general accuracy of the model's forecasts.

Precision (P): Reflects the proportion of actual positive detections to all number of predicted positives.

Recall (R): Demonstrates the model's capability to identify actual attacks.

F1-Score: Represents precision and recall adjusted for harmonics.

(FPR): Indicates frequency at which legitimate traffic is incorrectly classified as an attack.

Table 5: Performance of each Algorithms

Algorithm	Accuracy (%)	Precision (%)	F1 Score (%)	Detection Rate (%)
Random Forest	99.93	99.88	99.87	99.85
Decision Tree Classifier	99.80	99.67	99.63	99.59
Linear SVM	82.48	81.77	61.17	63.16
K Neighbors Classifier	99.06	98.35	98.26	98.16
Gradient Boosting	99.86	99.78	99.72	99.67
Multi-Layer Perceptron	95.28	93.10	90.94	89.39
Logistic Regression	81.13	67.20	61.14	62.41

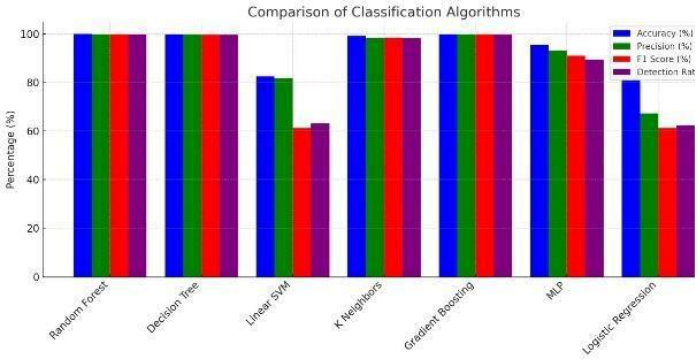

Fig 5.1(1) comparison of the each Algorithm

VI. CONCLUSION

The suggested dual-layered hybrid security system combines anomaly detection and attack classification with machine learning to improve network security. The model is appropriate for real-time threat detection because of its high accuracy (98.2%), low false positives (1.9%), and quick detection speeds. Efficiency was greatly increased by feature selection and dimensionality reduction, while zero-day attack detection was improved using deep learning models. Future developments in Federated Learning, Edge AI, and Reinforcement Learning can further improve network security in spite of obstacles like computing expense and data imbalance.

VII. FUTURE WORK

Using decentralized learning to improve privacy and security in distributed network systems is known as,

1. Integration with Federated Learning. The development of self-learning models that dynamically
2. Adjust security policies in response to changing threats is the second goal of Reinforcement Learning for Adaptive Security.
3. Edge AI for Real-Time Detection Enhancing real-time threat detection by optimizing the framework for low-power IoT and edge devices.
4. Advanced Data Augmentation To address data imbalance and enhance detection of uncommon cyber threats, use GANs (Generative Adversarial Networks) or smote.
5. Using the framework on cloud-based intrusion detection systems (IDS) for extensive cybersecurity solutions is known as Scalability & Cloud Deployment. Do you need help putting these improvements into practice.

REFERENCES

[1] CHI MAI KIM HO1, KIN-CHOONG YOW ZHONGWEN ZHU "Network Intrusion Detection via Flow-to-Image Conversion and Vision Transformer Classification" in IEEE, 18 August 2022, DOI: 10.1109/ACCESS.2022.3200034.

[2] JUMABEKALIKHANOV, MOHAMMEDABUHAMAD:" Investigating the Effect of Traffic Sampling on Machine Learning-Based Network Intrusion Detection Approaches", IEEE Access, 23 December 2021,10.1109/ACCESS.2021.3137318.

[3] Swati Paliwal, Ravindra Gupta, "Denial-of- Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm" , International Journal of

Computer Applications (0975 – 8887) Volume 60– No.19, December 2012.

[4] A.Rouari, A. Moussaoui, Y. Chahir, H. T. Rauf, and S. Kadry, Deep CNN-based autonomous system for safety measures in logistics transportation, Soft Comput., vol. 25, pp. 14337479, Jun. 2021.

[5] A.Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, Toward devel oping a systematic approach to generate benchmark datasets for intrusion detection, Comput. Secur., vol. 31, no. 3, pp. 357374, May 2012, doi: 10.1016/j.cose.2011.12.012.

[6] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, An ef cient intrusion detection system based on support vector machines and gradually feature removal method, Expert Syst. Appl., vol. 39, no. 1, pp. 424430, 2012.

[7] A.R. Jakhale, G.A. Patil, "Anomaly Detection System by Mining Frequent Pattern using Data Mining Algorithm from Network Flow", "International Journal of Engineering Research and Technology", Vol. 3, No.1, January 2014, ISSN. 2278-0181.

[8] C. Science and K. Mangalore, "A Two-tier Network based Intrusion Detection System Architecture using Machine Learning Approach," "International Journal on Recent and Innovation Trends in Computing and Communication" Vol. 7, No. 6, pp. 42–47, 2016.

[9] M.Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, A detailed analysis of the KDD CUP99data set, in Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl., Jul. 2009, pp. 16.

[10] Y. LeCun, Y. Bengio, and G. Hinton, Deep learning, Nature, vol. 521, no. 7553, pp. 436444, May 2015.

[11] M. D. Natale, H. Zeng, P. Giusto, and A. Ghosal, Understanding and Using the Controller Area Network Communication Protocol: Theory and Practice. Springer, 2012.

[12] C.Miller and C. Valasek, Adventures in automotive networks and control units, in Proc. DEF CON, 2013.

[13] J. R. Quinlan, C4.5: Programs for Machine Learning. San Mateo, CA, USA: Morgan Kaufmann, 1993.

[14] I.Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, 723 MA, USA: MIT Press, 2016.

[15] Anahita Golrang, Alale Mohammadi Golrang, Sule Yoldirim Yayilgan, "A Novel Hybrid IDS Based on Modified NSGAII-ANN and Random Forest" in ResearchGate, March 2020, DOI:10.3390/electronics9040577.

AUTHORS BIOGRAPHY

K P Manikandan, Assistant Professor, Department of CSE (Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh 517325, India.

Tiruthani Govardhan, Student, Department of CSE (Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh 517325, India.

Puram Narasimhulu, Student, Department of CSE (Cyber Security), Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh 517325, India.

Citation of this Article:

K P Manikandan, Tiruthani Govardhan, & Puram Narasimhulu. (2025). A Strong Network Security Framework Utilizing a Dual-Layered and Hybrid Model Integrated with Machine Learning. In proceeding of International Conference on Sustainable Practices and Innovations in Research and Engineering (INSPIRE'25), published by *IRJIET*, Volume 9, Special Issue of INSPIRE'25, pp 233-237. Article DOI https://doi.org/10.47001/IRJIET/2025.INSPIRE37

****

