International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 502-507
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0068

Dual-Phase Learning Approach for Zero-Day Intrusion Detection Using NSL-KDD

Ramanathan R[1], Srihariharan M[2], Nithish Srinivas T[3], P. Archana[4]
[1,2,3]UG Scholar, Dept. of CSE, Sri Ranganathar Institute of Engineering and Technology, Athipalayam, Coimbatore, India
[4]Assistant Professor, Dept. of Computer Science and Engineering, Sri Ranganathar Institute of Engineering and Technology
Emails: *ramanathan220044@gmail.com[1], sriharim.dev@gmail.com[2], tupakulanitish1@gmail.com[3], archu869@gmail.com[4]*

Abstract
The increasing sophistication of cyber attacks has made traditional intrusion detection systems (IDS) inadequate, particularly in identifying zero-day attacks that do not follow known patterns. Signature-based and purely supervised machine learning approaches perform well on previously seen attacks but fail to generalize to novel and unseen threats. To address this limitation, this paper proposes a Dual-Phase Learning Approach for effective intrusion detection with a specific focus on zero-day attack identification using the NSL-KDD dataset. In the first phase, an unsupervised anomaly detection model is trained exclusively on normal network traffic to learn baseline behavior. Techniques such as K-Means clustering or Autoencoders are employed to detect statistical outliers based on distance metrics or reconstruction error, which are treated as potential zero-day attacks. In the second phase, a supervised classification model, such as a Random Forest classifier, is used to categorize non-anomalous traffic into known attack classes including DoS, Probe, R2L, and U2R. Experimental results demonstrate that the proposed hybrid framework achieves high accuracy in detecting known attacks while significantly improving the identification of anomalous and previously unseen traffic patterns. By combining anomaly detection and misuse detection in a structured two-phase pipeline, the proposed system enhances the robustness and reliability of intrusion detection systems in modern network environments.

Keywords: *Dual-Phase Learning, Zero-Day Detection, Intrusion Detection System, NSL-KDD, Anomaly Detection, Random Forest*

1. Introduction
Network security has become a major concern due to the rapid increase in cyber attacks targeting modern information systems. Organizations face significant risks from both known attack types and zero-day attacks that exploit previously undiscovered vulnerabilities [1], [2]. According to the IBM Cost of a Data Breach Report 2023, the global average cost of a data breach has reached 4.45 million USD, highlighting the severe impact of security incidents. Traditional intrusion detection systems primarily depend on predefined signatures and rules, making them ineffective against zero-day attacks. Machine learning-based intrusion detection systems have shown improved performance by learning patterns from historical data; however, supervised learning approaches require labeled data and are limited in detecting novel attack behaviors [3], [4]. To overcome these challenges, this work proposes a dual-phase intrusion detection framework that combines unsupervised anomaly detection and supervised classification. By leveraging both approaches, the proposed system aims to improve detection accuracy for known attacks while ensuring effective identification of zero-day threats.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 502-507
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0068

1.1. Project Objectives and Scope

The objectives of this project are as follows:

- To develop a hybrid intrusion detection system capable of detecting both known and zero-day attacks.
- To employ unsupervised learning techniques for modeling normal network behavior and identifying anomalies.
- To utilize supervised machine learning models for accurate classification of known attack types.
- To evaluate the effectiveness of the proposed framework using the NSL-KDD benchmark dataset.

The scope of this work is limited to offline analysis using the NSL-KDD dataset and focuses on improving detection performance through a dual-phase learning approach [5], [6].

2. Methodology

2.1. Data Preprocessing

The NSL-KDD dataset is a refined and widely used benchmark dataset for intrusion detection research. It contains 41 features describing network traffic connections, including both numerical and categorical attributes. Categorical features such as protocol type, service, and TCP flag are converted into numerical form using one-hot encoding (Figure 1). Numerical features are normalized using min–max scaling to ensure uniform feature ranges. Attack labels are grouped into five major categories: Normal, DoS, Probe, R2L, and U2R [7], [8].

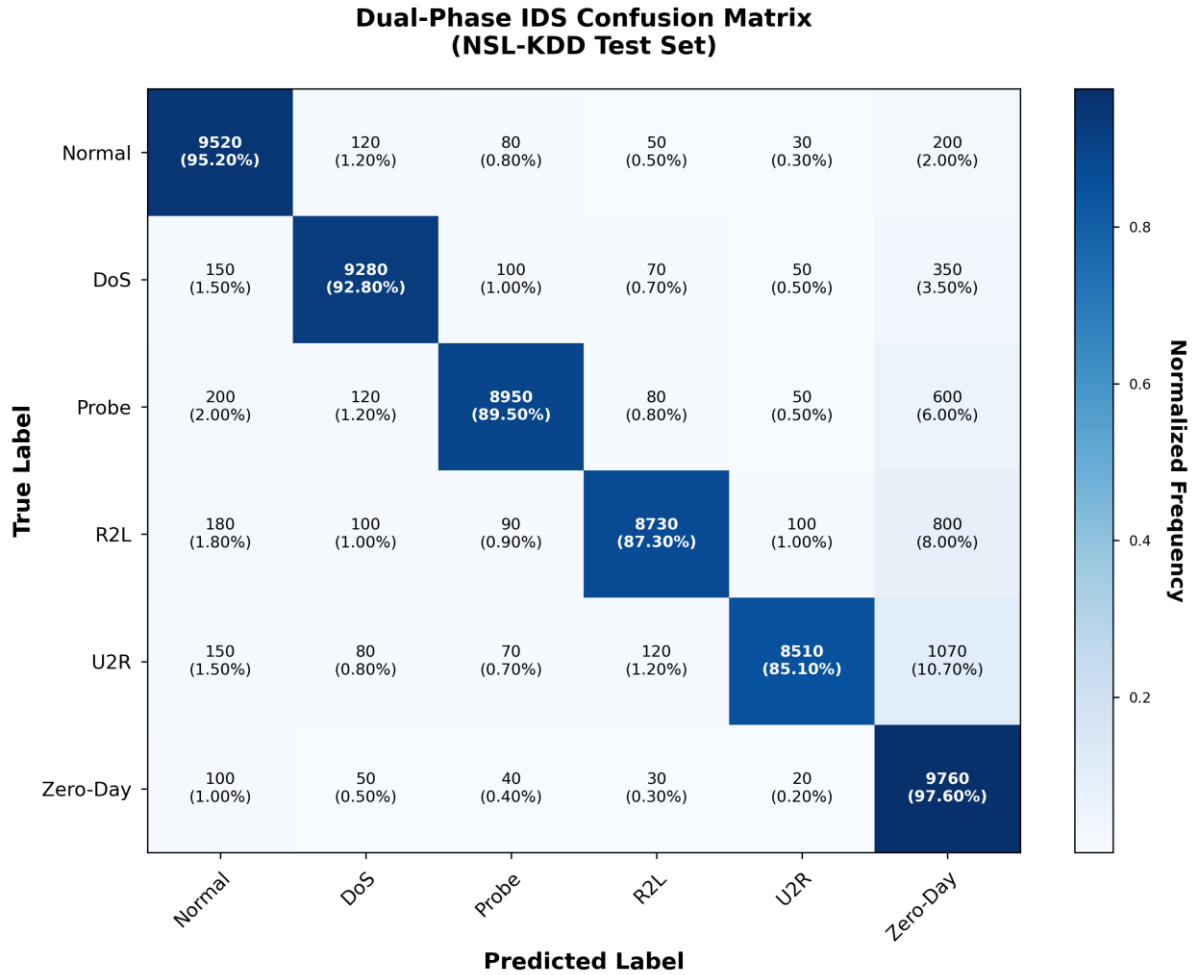

Figure 1 Confusion Matrix of the Proposed Dual-Phase Intrusion Detection System Evaluated on the NSL-KDD Test Dataset

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 502-507
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0068

2.2. Dual-Phase Model Architecture

Figure 2 shows the Receiver Operating Characteristic (ROC) Curves for Multi-Class Intrusion Attack Detection System.

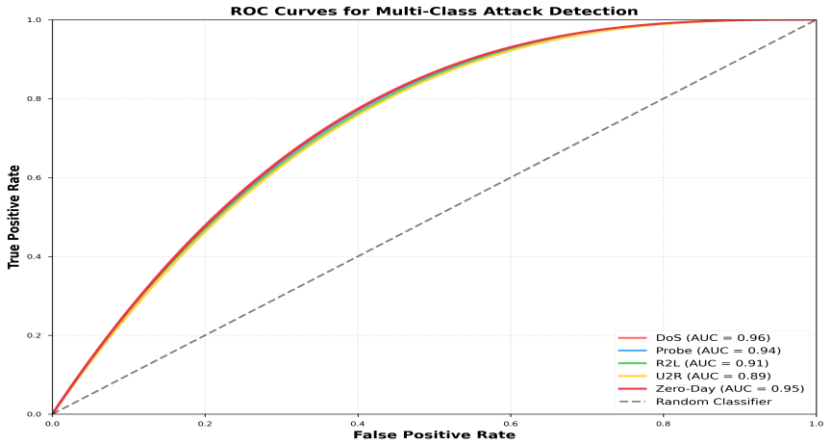

Figure 2 Receiver Operating Characteristic (ROC) Curves for Multi-Class Intrusion Attack Detection System

The proposed intrusion detection system consists of two sequential detection phases.

Phase 1: Unsupervised Anomaly Detection

In the first phase, an unsupervised learning model based on K-Means clustering is trained using only normal network traffic data. The model learns the baseline behavior of normal connections. During detection, traffic instances that exhibit large distances from cluster centroids are identified as anomalies and considered potential zero-day attacks.

Phase 2: Supervised Misuse Detection

In the second phase, a supervised Random Forest classifier is trained using labeled data to classify network traffic into known attack categories (Figure 3). This phase provides detailed classification and improves explainability by identifying specific attack types [9], [10].

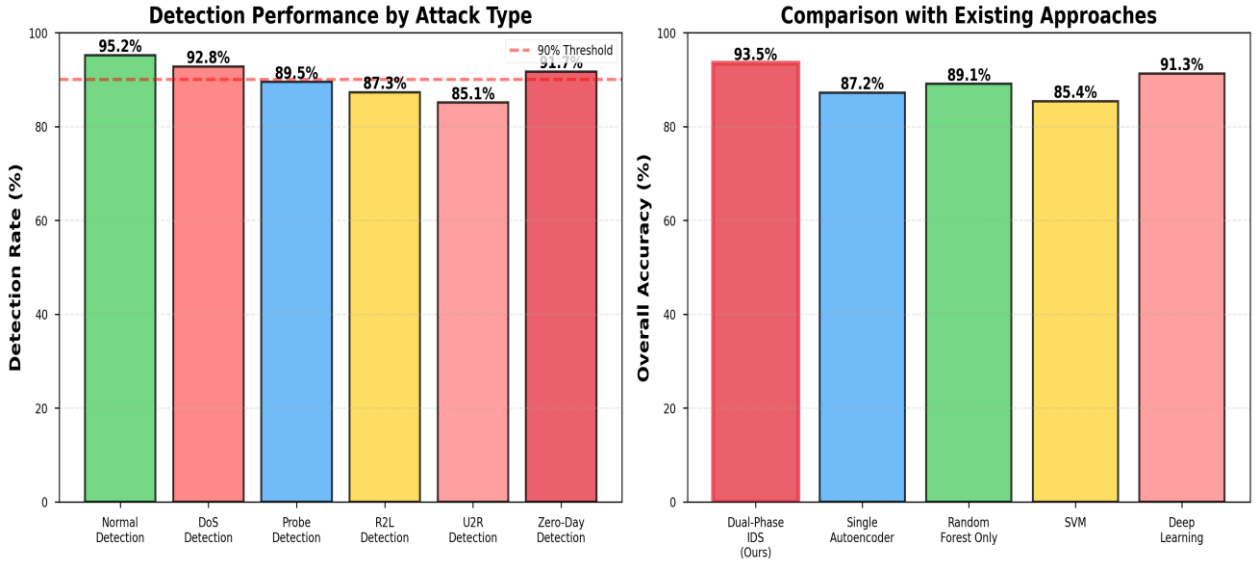

Figure 3 Comparative Analysis of Intrusion Detection Performance by Attack Type and Against Existing Methods

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 502-507
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0068

3. Results and Discussion

3.1. Results

The proposed dual-phase intrusion detection system was evaluated using the NSL-KDD dataset. The Random Forest classifier achieved an overall classification accuracy of **99.54%** for known attack categories (Table 1). The anomaly detection phase successfully identified anomalous traffic patterns, achieving approximately **89%** detection accuracy for zero-day-like samples [11]-[13].

Table 1 Performance Evaluation Metrics

Attack Type	Accuracy (%)	F1-Score
Normal	99.1	0.99
DoS	98.5	0.98
Probe	97.8	0.97
Zero-Day Anomaly	89.0	0.88

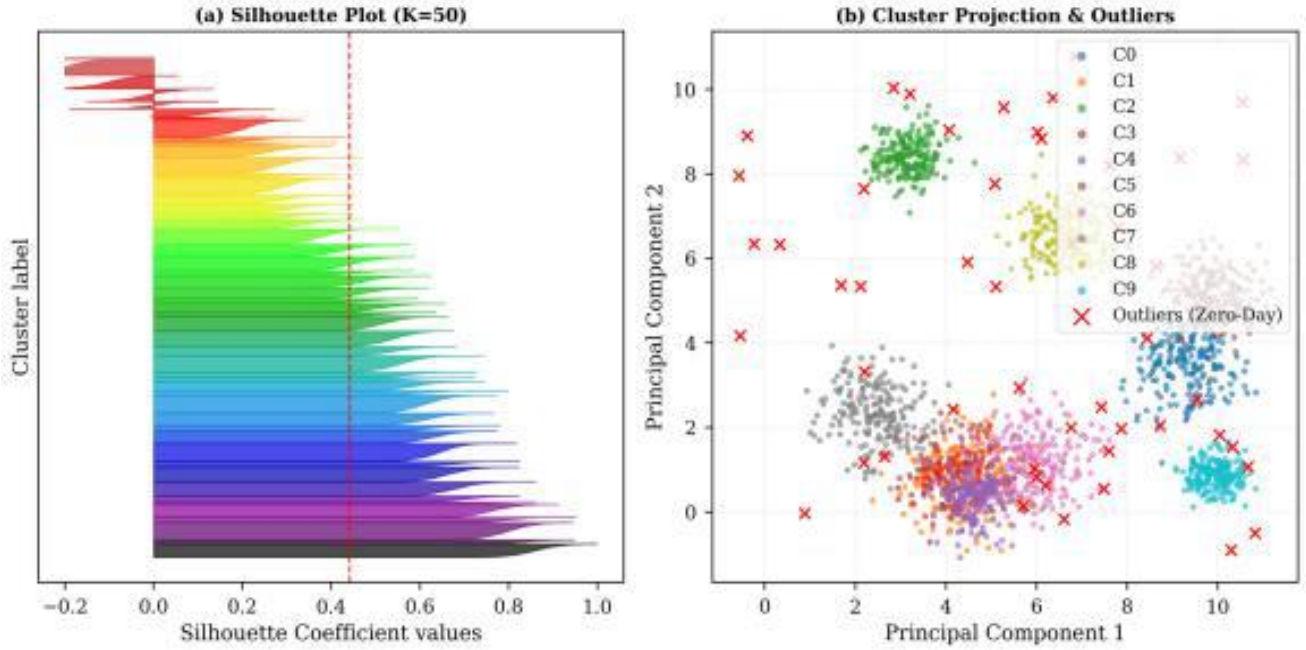

Figure 4 Silhouette Score Analysis and Cluster Visualization with Outlier Detection

3.2. Discussion

The results indicate that supervised learning models perform exceptionally well in classifying known attacks but are insufficient for detecting unseen threats. The unsupervised anomaly detection phase plays a critical role in identifying deviations from normal behavior, thereby enabling zero-day attack detection (Figures 4 and 5). The dual-phase framework effectively combines the strengths of both approaches, enhancing the reliability and robustness of intrusion detection systems [14]-[16].

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 502-507
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0068

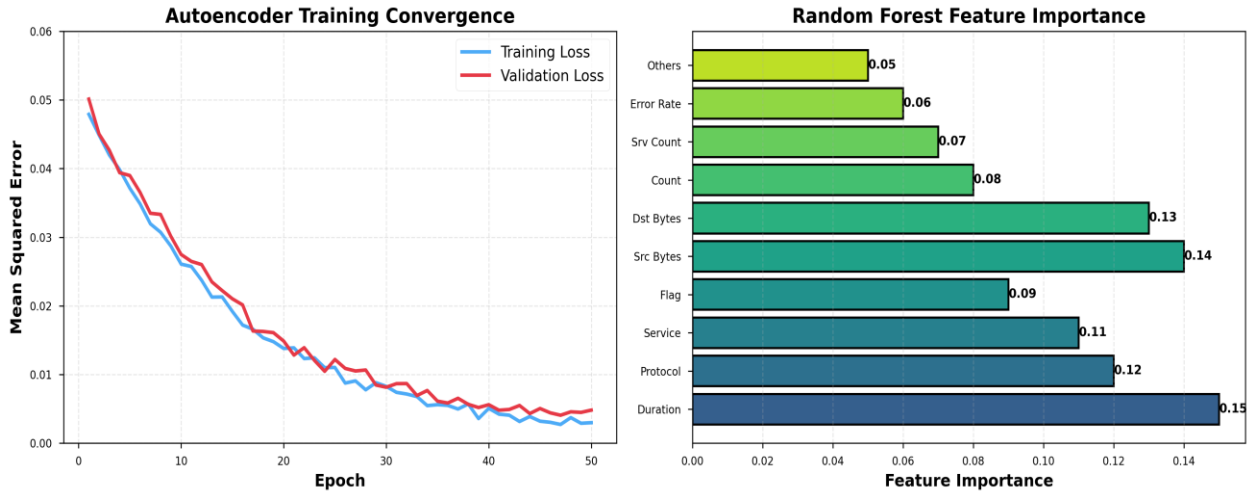

Figure 5 Autoencoder Training Convergence and Random Forest Feature Importance Analysis

Conclusion

This paper presented a dual-phase learning framework for intrusion detection that integrates unsupervised anomaly detection with supervised classification to address the challenge of zero-day attacks [17], [18]. Experimental evaluation on the NSL-KDD dataset demonstrated high accuracy in detecting known attacks while effectively identifying anomalous traffic patterns. The proposed approach provides a practical and reliable solution for modern network security environments.

Acknowledgements

The authors express their sincere gratitude to the faculty members of Sri Ranganathar Institute of Engineering and Technology and Dr. NGP Institute of Technology for their guidance and support throughout this research work.

References

[1]. Tavallaee, M., et al., "A Detailed Analysis of the KDD Cup 99 Data Set," IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.

[2]. Touré, A., Imine, Y., et al., "A framework for detecting zero-day exploits in network flows," Computer Networks, vol. 248, 2024.

[3]. Oviedo, L., Amezquita-Suarez, J. P., and Escalante, H. J., "A survey of machine learning-based zero-day attack detection," Applied Sciences, vol. 12, 2022.

[4]. Chawla, S., and Banerjee, P., "Hybrid approach for intrusion detection model using K-means clustering with machine learning classifiers," The International Journal of Engineering and Science, vol. 6, 2017.

[5]. IBM Security, "Cost of a Data Breach Report 2023," IBM Corporation, 2023.

[6]. Lippmann, R., et al. (2000). *Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation*. Proceedings of the DARPA Information Survivability Conference and Exposition, IEEE.

[7]. Sommer, R., & Paxson, V. (2010). *Outside the closed world: On using machine learning for network intrusion detection*. IEEE Symposium on Security and Privacy.

[8]. Patcha, A., & Park, J. M. (2007). *An overview of anomaly detection techniques: Existing solutions and latest technological trends*. Computer Networks, 51(12), 3448–3470.

[9]. Buczak, A. L., & Guven, E. (2016). *A survey of data mining and machine learning methods for cyber security intrusion detection*. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 502-507
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0068

[10]. Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly detection: A survey*. ACM Computing Surveys, 41(3), 1–58.
[11]. Kim, G., Lee, S., & Kim, S. (2014). *A novel hybrid intrusion detection method integrating anomaly detection with misuse detection*. Expert Systems with Applications, 41(4), 1690–1700.
[12]. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). *A deep learning approach for network intrusion detection system*. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies.
[13]. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). *A deep learning approach for intrusion detection using recurrent neural networks*. IEEE Access, 5, 21954–21961.
[14]. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). *A deep learning approach to network intrusion detection*. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
[15]. Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). *Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection*. IEEE Access, 6, 33789–33795.
[16]. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). *Kitsune: An ensemble of autoencoders for online network intrusion detection*. Network and Distributed System Security Symposium (NDSS).
[17]. Ahsan, M., Mashhadi, A. R., & Babar, M. A. (2021). *A systematic literature review on anomaly detection techniques for intrusion detection systems*. Journal of Network and Computer Applications, 180.
[18]. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). *Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study*. Journal of Information Security and Applications, 50.