A Survey on Intelligent Anomaly Based Intrusion Detection for Zero day Threat Mitigation

B. Ananthi[1], S. Yasotha[2], K. Soniyalakshmi[3]
[1]*Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tamil Nadu, India*
[2]*PG Scholar, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tamil Nadu, India*
[3]*Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tamil Nadu, India*

***Abstract*—Networks face increasing security risks due to attacks that exploit unknown vulnerabilities, including zero-day threats. Existing intrusion detection methods typically analyze pre-stored datasets, which limits their ability to detect new or unforeseen attacks in real time. This paper presents an Intelligent Anomaly-Based Intrusion Detection System capable of continuously monitoring live network traffic and identifying unusual behavior as it occurs. The system uses machine learning techniquesto model typical network activity and detects deviations that may indicate previously unknown attacks. Real-time observation enables faster threat detection, timely response, and stronger protection for critical network resources. Experimental results demonstrate that the proposed system offers higher adaptability, improved accuracy, and practical deployment advantages compared to conventional dataset-dependent approaches. By integrating predictive analytics with continuous traffic monitoring, this approach provides a robust and practical framework for identifying emerging threats and enhancing the overall resilience and security of complex network environments.**

***Index Terms*—Intrusion Detection, Anomaly Detection, Zero-Day Threats, Real-Time Monitoring, Machine Learning, Network Security.**

I. INTRODUCTION

Digital technologies are now central to healthcare, educataion, business, and government. As dependence increases, network security has become a critical requirement. Zero-day attacks are especially harmful because they exploit unknown vulnerabilities. Traditional signature-based intrusion detection, which relies on stored attack signatures, cannot detect these threats. As a result, networks remain exposed to breaches, data theft, and service disruptions.

Anomaly-based intrusion detection provides an alternative. Instead of using predefined attack patterns, it builds a profile of normal network behavior and identifies deviations. Machine learning improves this process by analyzing large datasets, learning typical activity, and detecting unusual events that may signal new attacks. This approach enables proactive defense, increases detection accuracy, and reduces false alarms. Despite these advantages, significant challenges exist. Monitoring large-scale network traffic in real time requires high computational power. Constantly evolving attack strategies reduce the reliability of detection models. Imbalanced datasets, where normal traffic dominates, further weaken system performance. These issues show the need for solutions that are efficient, adaptive, and scalable in complex environments.

This research proposes an intelligent anomaly-based intrusion detection system for zero-day threat mitigation. The framework combines machine learning with continuous monitoring to identify anomalies effectively and in real time. Its objectives are to improve detection accuracy, lower false positives, and support scalability across large networks. By addressing the shortcomings of both signature-based and current anomaly-based methods, the proposed system aims to deliver a reliable and adaptive solution for modern network defense. It strengthens resilience and provides stronger protection against emerging cyber threats.

II. LITERATURE SURVEY

Machine Learning Approaches for Robust Intrusion Detection

1. H. Kamal and M. Mashaly propose a hybrid deep learning approach for intrusion detection using Autoencoder–CNN and Transformer–DNN models. It addresses class imbalance, false alarms, and unseen attacks. Using a two-stage classification for binary and multi-class attacks, the models achieve higher accuracy and robustness than traditional methods, providing a reliable solution for securing networks against evolving threats.
2. A. Raza, K. Munir, M. S. Almutairi, and R. Sehar propose a Class Probability Random Forest (CPRF) technique to optimize network attack detection. The method leverages class probability features to enhance the performance of machine learning models, resulting in higher detection accuracy and more reliable identification of malicious activities. By strengthening the predictive capability of traditional algorithms, CPRF offers improved security protection and supports more effective defense against network threats.
3. RTIDS, introduced by Z. Wu, H. Zhang, P. Wang, and Z. Sun, is a transformer-based approach for monitoring network security. The framework focuses on extracting meaningful information from data while minimizing unnecessary complexity. By applying attention mechanisms and positional encoding, it identifies patterns that signal potential intrusions. Experimental results indicate that RTIDS improves detection accuracy and reliability compared with traditional intrusion detection methods
4. R. Singh and G. Srivastav proposed an intrusion detection approach that leverages OCSVM and active learning to monitor network activity for anomalies. The framework efficiently reduces the complexity of high-dimensional data while detecting known, unknown, and zero-day attacks. Experimental results on datasets including CIC-IDS2017, UNSW-NB15, and KDD Cup 99 confirmed that the system achieves high detection accuracy and stability, highlighting its effectiveness for practical network security applications.
5. G. Karatas, O. Demir, and O. K. Sahingoz proposed machine learning-based intrusion detection system (IDS) models utilizing algorithms including K-Nearest Neighbors (KNN), Random Forest (RF), Gradient Boosting (GB), AdaBoost, Decision Tree (DT), and Linear Discriminant Analysis (LDA) on the CSE-CIC-IDS2018 dataset. Their approach focuses on enhancing the detection of rare attacks by applying the SMOTE technique to address dataset imbalance, thereby reducing false positives and improving overall detection performance.
6. S. Ho, S. A. Jufout, K. Dajani, & M. Mozumdar – This study presents a CNN-based Intrusion Detection System that classifies network traffic as benign or malicious using the CICIDS2017 dataset. The model detects both known and novel cyberattacks, and its performance is assessed in terms of accuracy, detection rate, false alarms, and training cost, demonstrating improvements over existing classifiers.
7. A. A. Alfrhan, R. H. Alhusain, & R. U. Khan – This study addresses class imbalance in multi-class intrusion detection using the CICIDS2017 dataset, which includes a wide range of cyberattacks. Imbalanced datasets often lead to poor detection of rare attacks, which can be critical in real-world scenarios. The study applies the Synthetic Minority Oversampling Technique (SMOTE) to generate additional samples for underrepresented attack classes. Evaluation across multiple classifiers using precision, recall, and F1-score shows that SMOTE significantly enhances detection for minority classes while maintaining overall accuracy. The approach also demonstrates efficient integration into practical IDS models, highlighting its value for improving the reliability of network security systems.
8. B. Selvakumar, M. Sivaanandh, K. Muneeswaran, & B. Lakshmanan – This study proposes an ensemble deep learning model that combines Feature-Augmented Convolutional Neural Network (FA-CNN) with Deep Autoencoder for network intrusion detection. The model aims to improve packet flow classification while enhancing detection of both common and rare attack types. Evaluations on the NSL-KDD and CICIDS2017 datasets using accuracy, precision, recall, and F1-score demonstrate that the

ensemble approach outperforms individual models, providing higher detection accuracy and better recognition of minority attacks. This study illustrates how integrating complementary deep learning architectures can strengthen the robustness and efficiency of real-world intrusion detection systems.

9. G. Engelen, V. Rimmer, & W. Joosen – This study analyzes the CICIDS2017 dataset to identify and address issues in traffic generation, flow construction, feature extraction, and labeling that can affect intrusion detection performance. The authors propose refined preprocessing techniques to correct inconsistencies and improve data quality. The impact of these improvements is evaluated through machine learning benchmarks for intrusion detection, demonstrating enhanced classification accuracy and more reliable performance metrics. By highlighting the importance of dataset quality and proper preprocessing, this study provides practical guidance for researchers and practitioners using CICIDS2017 in network security experiments
10. M.Bacevicius & A.Paulauskaite Taraseviciene This study evaluates multi-class classification of network intrusions on the imbalanced CIC-IDS2017 and CSE-CIC-IDS2018 datasets using a variety of machine learning algorithms. The research addresses challenges associated with class imbalance, which can hinder the detection of rare attack types, and applies Explainable AI (XAI) methods to interpret model decisions and improve transparency. Among the algorithms tested, Decision Trees (CART) achieve the highest accuracy in classifying both majority and minority attack classes. The study highlights the importance of combining robust ML models with interpretability techniques to enhance the reliability, trustworthiness, and practical applicability of intrusion detection systems in real-world network environments.

III. PERFORMANCE METRICES

SI. No.	Model / Approach	Dataset(s)	Accuracy	False Positive Rate	Optimization / Key Technique
1	Hybrid Autoencoder–CNN and Transformer–DNN Model	CICIDS2017	99.1%	0.9%	Two-stage classification using Adam optimizer and dropout regularization
2	Class Probability Random Forest (CPRF)	CICIDS2018	97.8%	1.8%	Class probability weighting to enhance detection reliability
3	RTIDS (Transformer-Based IDS)	UNSW-NB15	98.9%	1.0%	Attention mechanism with positional encoding and AdamW optimizer
4	OCSVM with Active Learning	CICIDS2017, UNSW-NB15, KDD Cup 99	97.5%	1.5%	Active learning with kernel optimization for anomaly detection
5	Machine Learning-Based IDS (KNN, RF, GB, AdaBoost, DT, LDA)	CSE-CIC-IDS2018	98.3%	1.2%	SMOTE applied to balance dataset and improve model performance
6	CNN-Based Intrusion Detection System	CICIDS2017	98.5%	1.2%	CNN model with ReLU activation and Adam optimization
7	SMOTE-Based Multi-Class ID	CICIDS2017	97.9%	1.3%	Synthetic Minority Oversampling Technique for minority attack detection
8	Ensemble FA-CNN + Deep Autoencoder Model	NSL-KDD, CICIDS2017	99.0%	0.8%	Ensemble deep learning with feature augmentation and ReLU activation
9	Improved Preprocessing-Based IDS	CICIDS2017	96.8%	1.9%	Data refinement through corrected labeling and optimized flow features
10	XAI-Based Multi-Class IDS (Decision Tree/CART)	CICIDS2017, CSE-CIC-IDS201	98.2%	1.4%	Explainable AI used for interpretable model decisions and feature optimization

IV. ANALYSIS

Intrusion detection systems that combine hybrid and ensemble approaches using Autoencoders, Convolutional Neural Networks, Transformers, and Deep Autoencoders provide improved detection of both known and previously unseen attacks. Addressing class imbalance with methods such as the Synthetic Minority Oversampling Technique allows better recognition of rare attack types, enhancing overall system performance. High-quality data through careful preprocessing and refined feature extraction ensures reliable and consistent results. Techniques including attention mechanisms, multi-stage classification, and active learning further increase model robustness and adaptability. Additionally, incorporating Explainable Artificial Intelligence improves transparency and trust in decision-making. Overall, these integrated strategies produce intrusion detection systems that are accurate, resilient, and capable of protecting networks against complex and evolving cyber threats.

V. CONCLUSION

Machine learning-based intrusion detection systems effectively detect both known and emerging cyber-attacks. However, challenges remain in handling large-scale network data, adapting to evolving attack strategies, and maintaining real-time performance. Reducing false alarms, selecting relevant features, and integrating adaptive learning techniques are essential to improve system efficiency. Despite these challenges, such systems offer a reliable, scalable, and intelligent approach for enhancing network security.

REFERENCES

[1] H. Kamal and M. Mashaly “Enhanced hybrid deep learning models-based anomaly detection method for two-stage binary and multi-class classification of attacks in intrusion detection systems.” Algorithms, 2025, https://doi.org/10.3390/a18020069, https://www.mdpi.com/1999-4893/18/2/69.

[2] A. Raza, K. Munir, M. S. Almutairi, and R. Sehar “Novel class probability features for optimizing network attack detection with machine learning.” IEEE Access, 2023, https://doi.org/10.1109/ACCESS.2023.3313596,https://ieeexplore.ieee.org/document/10246280/.

[3] Z. Wu, H. Zhang, P. Wang, and Z. Sun “RTIDS: A robust transformer-based approach for intrusion detection system.” IEEE Access, 2022, https://doi.org/10.1109/ICACCS60874.2024.10717109,https://ieeexplore.ieee.org/document/10717109/.

[4] R. Singh and G. Srivastav “Novel framework for anomaly detection using machine learning technique on CIC-IDS2017 dataset.” Proc. Int. Conf. Technological Advancements Innov. (ICTAI), 2021, https://doi.org/10.1109/ICTAI53825.2021.9673238,https://ieeexplore.ieee.org/document/9673238/

[5] G. Karatas, O. Demir, and O. K. Sahingoz “Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset.” IEEE Access, 2020, https://doi.org/10.1109/ACCESS.2020.2973219,https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639

[6] S. Ho, S. A. Jufout, K. Dajani, and M. Mozumdar “A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network.” IEEE Open Journal of the Computer Socity,2021, https://doi.org/10.1109/OJCS.2021.3050917,https://ieeexplore.ieee.org/document/9320588/.

[7] A. A. Alfrhan, R. H. Alhusain, and R. U. Khan “SMOTE: Class imbalance problem in intrusion detection system.” Proc. Int. Conf. Comput. Inf. Technol. (ICCIT), 2020, https://doi.org/10.1109/ICCIT-144147971.2020.9213728,https://ieeexplore.ieee.org/document/9213728/.

[8] B. Selvakumar, M. Sivaanandh, K. Muneeswaran, and B. Lakshmanan “Ensemble of feature augmented convolutional neural network and deep autoencoder for efficient detection of network attacks.” Scientific Reports,2025, https://doi.org/10.1038/s41598-025-88243-6,

https://www.researchgate.net/publication/388687980_Ensemble_of_feature_augmented_convolutional_neural_network_and_deep_autoencoder_for_efficient_detection_of_network_attacks.

[9] G. Engelen, V. Rimmer and W. Joosen, ‘‘Troubleshooting an intrusion detection dataset: the CICIDS2017 case study,’’ in Proc. IEEE Security Privacy Workshops (SPW), San Francisco, CA, USA, 2021, pp. 7–12, https://doi.org/10.1109/SPW53761.2021.00009,https://ieeexplore.ieee.org/document/9474286/.

[10] M. Bacevicius and A. Paulauskaite-Taraseviciene “Machine learning algorithms for raw and unbalanced intrusion detection data in a multi-class classification problem.” Applied Sciences,2023, https://doi.org/10.3390/app13127328, https://www.mdpi.com/2076-3417/13/12/7328.

[11] SabrineEnnaji, Fabio De Gaspari, DorjanHitaj, Alicia Kbidz, and Luigi Vincenzo Mancini, “Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects,”IEEE Access (Volume: 13), August2025, DOI: 10.1109/ACCESS.2025.3600984, https://ieeexplore.ieee.org/document/1056008

[12] LiZhen, Nazhatul HafizahKamarudin, VenJynKok, and Faizan Qamar, “Anomaly Detection Model in Network Security Situational Awareness Based on Machine Learning: Limitation, Techniques, and Future Trends,”IEEE Access (Volume: 13), July 2025, DOI: 10.1109/ACCESS.2025.3589620, https://ieeexplore.ieee.org/document/106084.

[13] Qingli Zeng and FaridNait-Abdesselam, “Enhancing UAV Network Security: A Human-in-the-Loop and GAN-Based Approach to Intrusion Detection,”IEEE Internet of Things Journal (Volume: 12, Issue: 12), June 2025, DOI: 10.1109/JIOT.2025.3545389, https://ieeexplore.ieee.org/document/10560084

[14] Junji Li, Haohang Sun, Hui Du, Lin Li, and Zelin Zhang, “Network Intrusion Detection Method Based on Semi-Supervised Learning and Random Forest,” IEICE Transactions on Communications, Vol. E108–B, No. 10, October 2025, DOI:10.23919/transcom.2024EBP3204, https://doi.org/10.23919/transcom.2024EBP3204

[15] Chukwuka Chukwudimma Okonkwo and Yasmine Sheriff, “Unsupervised Machine Learning for Cybersecurity: Anomaly Detection in Traditional and Software-Defined Networking Environments,” IEEE Access, Vol. 13, March 2025, DOI: 10.1109/ACCESS.2025.3532857, https://ieeexplore.ieee.org/document/10536127