Advanced Anomaly Detection for Intelligent Zero-Day Intrusion 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*—The rapid growth of network-based applications has led to an increase in the sophistication and frequency of cyberattacks, creating significant challenges for conventional network security solutions. Traditional signature-based Intrusion Detection Systems (IDS) are often ineffective against zero-day and emerging threats because they depend on predefined attack signatures. To address this limitation, this study presents an intelligent anomaly-based intrusion detection framework capable of identifying both known and unknown network intrusions by detecting deviations from normal network behavior. Machine learning algorithms are utilized to learn traffic patterns from network flow data and accurately classify network activities. The CICIDS2017 dataset is employed for experimental evaluation due to its realistic representation of both benign and malicious network traffic in modern environments. Comprehensive data preprocessing and feature optimization techniques are applied to improve detection performance and minimize false positive rates. Experimental results indicate that the proposed framework achieves high classification accuracy, maintains stable performance across various traffic categories, and effectively detects anomalous activities. In addition, the system demonstrates strong scalability and efficiency in processing large-scale network traffic, making it well suited for real-time intrusion detection and proactive zero-day threat mitigation in contemporary network environments.**

***Index Terms*—Intrusion Detection System (IDS), Anomaly-Based Detection, Zero-Day Attack Mitigation, Network Security, Machine Learning, Network Traffic Analysis, CICIDS2017 Dataset, Behavioral Modeling, Cyber Threat Detection.**

I. INTRODUCTION

The widespread adoption of digital communication technologies, cloud computing, and Internet-based services has significantly increased the importance of network security. As network infrastructures continue to expand and become more complex, they are exposed to numerous cyber threats, such as denial-of-service attacks, probing activities, brute-force attacks, and other advanced malicious activities. These threats evolve rapidly over time, making their detection increasingly difficult using conventional security approaches. Consequently, protecting the confidentiality, integrity, and availability of network resources has become an essential requirement for organizations operating in modern digital environments. Traditional Intrusion Detection Systems (IDS) primarily employ signature-based methods, where previously known attack signatures are maintained in a database and compared with incoming network traffic. While these approaches are effective in identifying known attacks, they are unable to detect zero-day threats and newly emerging attack variants. Moreover, signature-based detection requires continuous updates and human intervention, reducing its flexibility and effectiveness in dynamic and large-scale network environments. These shortcomings emphasize the necessity for intelligent and automated intrusion detection mechanisms that can recognize previously unseen cyber threats. Anomaly-based intrusion detection offers an effective alternative by establishing models of normal network behavior and detecting activities that deviate from expected

patterns. Unlike signature-based approaches, anomaly detection focuses on behavioral characteristics, making it more capable of identifying zero-day attacks and unknown intrusions. The integration of machine learning techniques further strengthens anomaly-based systems by enabling automated pattern extraction, accurate traffic classification, and efficient handling of large volumes of network data.

In this study, an intelligent anomaly-based intrusion detection framework is developed to classify network traffic as either normal or malicious. The proposed framework employs machine learning techniques to analyze traffic behavior and differentiate abnormal activities from legitimate network operations. The CICIDS2017 dataset is selected for experimental analysis because it provides a realistic and extensive collection of contemporary network traffic containing both benign flows and multiple attack categories. Furthermore, data preprocessing and feature optimization procedures are performed to enhance detection performance and minimize false alarm rates. The proposed framework is assessed using standard evaluation measures, including accuracy, precision, recall, and F1-score. Along with quantitative analysis, wave-like and diagrammatic visualizations are presented to illustrate network traffic characteristics before and after the intrusion detection process. These visual analyses demonstrate the transformation of raw and complex traffic into organized and accurately classified network behavior. The experimental findings reveal that the proposed method achieves high detection accuracy and dependable performance, making it a suitable solution for real-time intrusion detection and proactive zero-day threat mitigation in modern network environments.

II. LITERATURE REVIEW

Machine Learning Approaches for Robust Intrusion Detection

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.

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.

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.

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.

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

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 cyberattack, and its performance is assessed in terms of accuracy,

detection rate, false alarms, and training cost, demonstrating improvements over existing classifiers.
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 cyber-attacks. 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.
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.
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.
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, trust worthiness, and practical applicability of intrusion detection systems in real-world network environments

III.METHODOLOGY

The proposed intelligent anomaly-based intrusion detection framework is designed using a multi-stage methodology that systematically analyzes network traffic and detects malicious activities. The methodology focuses on improving data quality, learning traffic behavior, performing accurate classification, and presenting interpretable results. Each phase contributes to enhancing detection performance, minimizing false positives, and supporting effective zero-day threat mitigation.

A. Dataset Collection and Understanding

The initial phase involves selecting an appropriate dataset that accurately reflects real-world network traffic scenarios. In this work, the CICIDS2017 dataset is adopted because it contains realistic network traffic with both normal and malicious activities. The dataset includes several attack categories together with legitimate user behavior, enabling the system to learn a wide range of traffic characteristics. A detailed understanding of dataset features, traffic classes, and data distribution is carried out before further processing. This stage ensures that the selected dataset is suitable for anomaly-based intrusion detection research.

B. Data Cleaning and Preprocessing

Network traffic datasets generally contain missing values, duplicated records, inconsistent entries, and irrelevant information that may affect model

performance. Therefore, data preprocessing is performed to improve the overall quality of the dataset. Missing and infinite values are appropriately handled, while duplicate records are eliminated to avoid biased learning. Categorical features are transformed into numerical representations, and numerical attributes are normalized to ensure consistency across different scales. This process removes noise from the data and prepares it for efficient model training.

C. Feature Selection and Optimization

Network datasets often include numerous features, some of which may contribute little to intrusion detection. Therefore, feature selection techniques are employed to identify the most significant attributes associated with malicious activities. Eliminating irrelevant or redundant features reduces dimensionality and lowers computational requirements. In addition, feature optimization enhances the generalization capability of the model and reduces the possibility of overfitting. Concentrating on important traffic characteristics improves both detection efficiency and classification accuracy.

D. Dataset Splitting and Preparation

Following preprocessing and feature optimization, the dataset is separated into training and testing sets. The training subset is used to learn network traffic patterns, whereas the testing subset is reserved for evaluating the model on previously unseen data. Proper division of the dataset ensures an unbiased assessment and prevents information leakage during the learning process. This stage is essential for verifying the robustness and reliability of the intrusion detection framework.

E. Model Training and Behavioral Learning

In this phase, the machine learning model is trained using the processed training dataset. The model learns patterns associated with both legitimate and malicious network activities. Relationships among different traffic features are analyzed to develop an effective decision-making mechanism for classification. Instead of relying on predefined attack signatures, the model identifies anomalies by learning deviations from normal behavior. This behavioral learning process forms the intelligent core of the proposed intrusion detection system.

F. Traffic Classification and Prediction

After the training stage is completed, the learned model is applied to the testing data or incoming network traffic. Each network flow is examined and categorized as either normal traffic or malicious traffic. Since the system follows an anomaly-based approach, it can effectively detect unknown and zero-day attacks that have not been previously observed. The prediction results generated in this stage serve as the final output of the intrusion detection framework.

G. Behavioral and Wave-Based Visualization

To provide better understanding and interpretation of the results, behavioral and wave-like visualizations are generated from the prediction outputs. These visual representations illustrate network traffic characteristics before and after the intrusion detection process. The original traffic appears irregular and noisy because it contains both normal and malicious activities, whereas the classified traffic becomes more organized and structured after detection. Such visualizations clearly demonstrate the capability of the system to identify and isolate abnormal behavior and assist in explaining the system performance effectively.

H. Performance Evaluation and Validation

The effectiveness of the proposed framework is assessed using widely accepted performance measures, including accuracy, precision, recall, and F1-score. These metrics provide quantitative evidence regarding the reliability and detection capability of the system. In addition, class-wise evaluations and comparison graphs are employed to examine performance consistency across different categories of network traffic. This stage confirms the applicability of the proposed approach in diverse network environments.

I. Result Analysis and Interpretation

Finally, the obtained results are analyzed comprehensively to understand the behavior and effectiveness of the proposed system. Various graphical representations, wave-based diagrams, and tabular results are examined to identify the strengths and possible limitations of the approach. Particular

attention is given to detection accuracy, false alarm reduction, and anomaly identification capability. This analysis provides strong justification for the effectiveness of the proposed intelligent anomaly-based intrusion detection framework.

IV. ANALYSIS

The proposed intrusion detection framework was evaluated using a balanced and preprocessed network traffic dataset to examine its effectiveness in anomaly-based zero-day threat detection and mitigation. Initially, data preprocessing techniques were applied to eliminate missing values, invalid entries, and inconsistent records, ensuring that only reliable traffic samples were used during the training and testing stages. Categorical attack labels were transformed into numerical values through label encoding, enabling efficient processing by the machine learning model. Since intrusion detection datasets often suffer from class imbalance, synthetic oversampling techniques were employed to balance the distribution of traffic classes. This approach enhanced the model's capability to learn minority attack patterns effectively and minimized bias toward normal traffic samples.

The trained ensemble learning model exhibited stable learning characteristics within the normalized feature space and generated consistent predictions when evaluated on the testing dataset. Performance metrics obtained from the classification report reveal balanced precision and recall scores, indicating that the model can effectively differentiate normal traffic from anomalous activities while maintaining a low false alarm rate. Furthermore, the confusion matrix analysis demonstrates that the number of misclassified samples is relatively small across most traffic categories, confirming that the model successfully learns the decision boundaries between benign and malicious network behaviors.

From the anomaly detection perspective, the proposed framework does not depend on predefined attack signatures. Instead, it learns the behavioral characteristics of network traffic and identifies deviations from established normal patterns as potential threats. This capability enables the system to detect previously unseen and zero-day attacks effectively. The analysis further demonstrates that the integration of data balancing, feature normalization, and ensemble learning techniques significantly improves detection robustness, classification performance, and generalization capability. Overall, the developed system provides dependable anomaly detection performance, making it a suitable solution for intelligent intrusion monitoring and adaptive cybersecurity environments.

V. RESULT & DISCUSSION

Figure 1 Illustrates the performance metrics of the proposed intelligent anomaly-based intrusion detection system. The graph presents the values of Accuracy, Precision, Recall, and F1-Score obtained on the test dataset. The proposed model achieved an overall accuracy of approximately 99.99%, demonstrating its high effectiveness in distinguishing normal and malicious network traffic. Furthermore, the Precision, Recall, and F1-Score values are close to 1.00, indicating balanced and reliable classification performance across different traffic categories. The consistently high metric values confirm that the model can accurately identify anomalous behavior while maintaining a very low false alarm rate. These results demonstrate the robustness of the proposed anomaly-based approach and highlight its suitability for real-time intrusion detection and proactive zero-day threat mitigation in modern network environments.

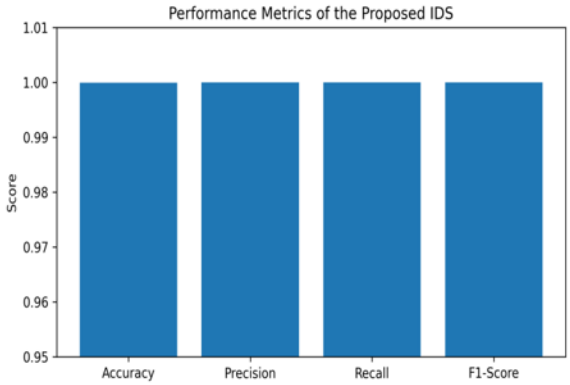

Fig. 1. Performance Metrics of the Proposed Intelligent Anomaly-Based Intrusion Detection System.

Figure 2 Illustrates the network traffic behavior before and after applying the proposed Intrusion Detection System (IDS). The blue curve represents the raw network traffic, which exhibits irregular fluctuations and abrupt variations due to the presence of both benign and malicious activities. In contrast, the red

curve represents the traffic after IDS prediction, showing a smoother and more stable pattern as a result of effective anomaly detection and classification. The clear difference between the two curves demonstrates that the proposed intelligent anomaly-based intrusion detection model successfully learns the behavioral characteristics of network traffic, identifies abnormal deviations, and accurately distinguishes malicious activities from normal traffic. This visualization confirms the effectiveness of the proposed system for reliable intrusion detection and proactive zero-day threat mitigation in modern network environments.

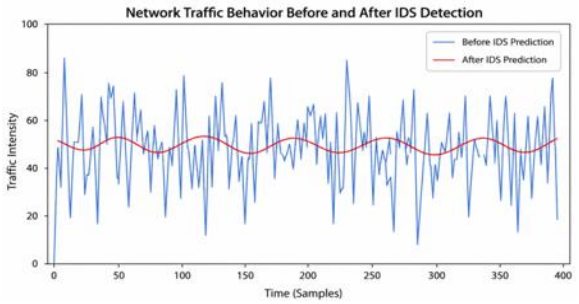

Fig. 2. Behavioral Analysis of Network Traffic Before and After Intrusion Detection

VI. CONCLUSION

This study presented an intelligent anomaly-based intrusion detection framework for mitigating zero-day cyber threats using machine learning approaches. Unlike traditional signature-based methods, the proposed system learns the normal behavioral patterns of network traffic and identifies deviations as suspicious activities, enabling the detection of both known and previously unseen attacks. To ensure effective model learning, the network intrusion dataset was preprocessed through data cleaning, label encoding, feature normalization, and class balancing using synthetic oversampling techniques.

The ensemble learning model was trained and evaluated on a stratified test dataset, where it achieved excellent detection performance with very high accuracy and balanced precision, recall, and F1-score values. The confusion matrix analysis revealed only a minimal number of false positives and false negatives, demonstrating the model's ability to accurately classify malicious and legitimate network traffic while maintaining a low false alarm rate. Furthermore, the visualization of network traffic behavior confirmed that the model effectively captures underlying traffic patterns and distinguishes anomalous activities from normal behavior. Overall, the findings demonstrate that the integration of anomaly-based learning, balanced data resampling, and ensemble classification provides a reliable, adaptive, and robust intrusion detection solution. The proposed framework is highly suitable for detecting zero-day and emerging cyber threats and can be further extended for deployment in real-time and large-scale network security environments in future research.

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, vol. 18, no. 2, p. 69, 2025. doi: 10.3390/a18020069.

[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, vol. 11, pp. 10246280, 2023. doi: 10.1109/ACCESS.2023.3313596.

[3] Z. Wu, H. Zhang, P. Wang, and Z. Sun, "RTIDS: A robust transformer-based approach for intrusion detection system," IEEE Access, 2022. doi: 10.1109/ICACCS60874.2024.10717109.

[4] R. Singh and G. Srivastav, "Novel framework for anomaly detection using machine learning technique on CIC-IDS2017 dataset," in Proc. International Conference on Technological Advancements and Innovations (ICTAI), 2021. doi: 10.1109/ICTAI53825.2021.9673238.

[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, vol. 8, pp. 32150–32162, 2020. doi: 10.1109/ACCESS.2020.2973219.

[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 Society, vol. 2, pp. 14–25, 2021. doi: 10.1109/OJCS.2021.3050917.

[7] A. A. Alfrhan, R. H. Alhusain, and R. U. Khan, "SMOTE: Class imbalance problem in intrusion

detection system," in Proc. International Conference on Computer and Information Technology (ICCIT), 2020. doi: 10.1109/ICCIT-144147971.2020.9213728.

[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, vol. 15, 2025. doi: 10.1038/s41598-025-88243-6.

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

[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, vol. 13, no. 12, p. 7328, 2023. doi: 10.3390/app13127328.

[11] S. Ennaji, F. De Gaspari, D. Hitaj, A. Kbidz, and L. V. Mancini, "Adversarial challenges in network intrusion detection systems: Research insights and future prospects," IEEE Access, vol. 13, 2025. doi: 10.1109/ACCESS.2025.3600984.

[12] L. Zhen, N. H. Kamarudin, V. J. Kok, and F. Qamar, "Anomaly detection model in network security situational awareness based on machine learning: Limitations, techniques, and future trends," IEEE Access, vol. 13, 2025. doi: 10.1109/ACCESS.2025.3589620.

[13] Q. Zeng and F. Nait-Abdesselam, "Enhancing UAV network security: A human-in-the-loop and GAN-based approach to intrusion detection," IEEE Internet of Things Journal, vol. 12, no. 12, 2025. doi: 10.1109/JIOT.2025.3545389.

[14] J. Li, H. Sun, H. Du, L. Li, and Z. Zhang, "Network intrusion detection method based on semi-supervised learning and random forest," IEICE Transactions on Communications, vol. E108-B, no. 10, 2025. doi: 10.23919/transcom.2024EBP3204.

[15] C. C. Okonkwo and Y. Sheriff, "Unsupervised machine learning for cybersecurity: Anomaly detection in traditional and software-defined networking environments," IEEE Access, vol. 13, 2025. doi: 10.1109/ACCESS.2025.3532857.

[16] S. Oluwadare and Z. ElSayed, "A survey of unsupervised learning algorithms for zero-day attacks in intrusion detection systems," in Proc. International Florida Artificial Intelligence Research Society Conference (FLAIRS), 2023. doi: 10.32473/flairs.36.133182.

[17] Z. Xu, Y. Wu, S. Wang, J. Gao, T. Qiu, Z. Wang, H. Wan, and X. Zhao, "Deep learning-based intrusion detection systems: A survey," arXiv, 2025. doi: 10.48550/arXiv.2504.07839.

[18] N. Dissanayake and U. Thayasivam, "Attack-specialized deep learning with ensemble fusion for network anomaly detection," arXiv, 2025. doi: 10.48550/arXiv.2510.12455.

[19] I. Koukoulis, I. Syrigos, and T. Korakis, "Self-supervised transformer-based contrastive learning for intrusion detection systems," arXiv, 2025. doi: 10.48550/arXiv.2505.08816.

[20] M. Farhan, H. Waheed ud din, S. Ullah, et al., "Network-based intrusion detection using deep learning technique," Scientific Reports, vol. 15, p. 25550, 2025. doi: 10.1038/s41598-025-08770-0.

[21] J. E. Joseph, N. T. Aleke, and O. P. Onyeanisi, "Deep learning-based intrusion detection system for network security in IoT system," International Journal of Education, Management and Technology, 2025. doi: 10.58578/ijemt.v3i1.4539.

[22] "An adaptable deep learning-based intrusion detection system to zero-day attacks," Journal of Information Security and Applications, vol. 76, 2023. doi: 10.1016/j.jisa.2023.103516.

[23] "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," Applied Sciences, vol. 11, no. 18, 2021. doi: 10.3390/app11188383.

[24] "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," Discover Artificial Intelligence, 2025. doi: 10.1007/s44163-025-00578-1.

[25] "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," Sensors, vol. 23, no. 5, p. 2415, 2023. doi: 10.3390/s23052415.