Proceedings of the 5th International Conference on Pervasive Computing and Social Networking (ICPCSN-2025)
IEEE Xplore Part Number: CFP25EZ5-ART; ISBN: 979-8-3315-3519-3

Detecting Zero-Day Attacks using Advanced Anomaly Detection in Network Traffic

[1]Dr Asma Anjum
Assistant Professor
Computer Science and Engineering
HKBK College of Engineering, Bangalore
asmacs13@gmail.com

[2]P. Rama Subramanian
Assistant professor
Computer Science and Engineering
P.S.R engineering college, Sivakasi
Ramboga29@gmail.com

[3]R.Stalinbabu
Assistant Professor
Artificial Intelligence and Machine Learning
M.Kumarasamy College of Engineering, Karur
rstalinbabu@gmail.com

[4]Dr.Deepthi Kothapeta
Assistant professor
Computer science and Artificial Intelligence
SR University,
k.deepthi@sru.edu.in

[5]K.Santha Sheela
Assistant Professor
Department of CSE
Velammal College of engineering and technology
sheelakodi@gmail.com

[6]Dr.B.Jegajothi
Research Associate
SRS Tech Solutions
Chennai
jegajothibalakrishnan@gmail.com

2025 5th International Conference on Pervasive Computing and Social Networking (ICPCSN) | 979-8-3315-3519-3/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICPCSN65854.2025.11034868

***ABSTRACT*-Zero-day attacks pose a significant challenge to cybersecurity due to their unpredictable nature and the lack of labeled attack data for training conventional detection models. This research proposes a Hybrid Deep Anomaly Detection Model that integrates Autoencoders, Transformer-Based Detection, and Isolation Forest to enhance the identification of zero-day attacks in network traffic. The Autoencoder component learns normal traffic patterns and identifies deviations based on reconstruction errors. A Transformer-based model captures temporal dependencies in network traffic using self-attention mechanisms, improving the representation of evolving attack behaviors. Finally, an Isolation Forest refines anomaly detection by isolating outliers and reducing false positives. The model is trained and evaluated on the CSE-CIC-IDS2018 dataset, which contains diverse cyberattack scenarios, ensuring a robust performance assessment. The results of the proposed model achieve 97.2% accuracy and a false positive rate of 2.8%, significantly outperforming existing approaches such as Autoencoder-only, LSTM-based detection, and Random Forest classifiers. The proposed framework enhances zero-day attack detection, minimizes false alerts, and ensures real-time adaptability in modern cybersecurity environments.**

KEYWORDS— Hybrid Deep Learning, Anomaly Detection, Zero-Day Attack, Autoencoder, Transformer Model, Isolation Forest, Intrusion Detection, Network Security, Feature Learning.

I. INTRODUCTION

The rapid growth of digital infrastructure has led to a significant increase in network connectivity, enabling seamless communication and information exchange across the globe [1]. However, this increased connectivity has also exposed networks to advanced cyber threats, with zero-day attacks emerging as one of the most critical security challenges. Zero-day attacks exploit unknown vulnerabilities, allowing attackers to bypass traditional security mechanisms before patches or countermeasures can be deployed. These attacks pose severe risks, including unauthorized data access, service disruptions, and financial losses, making them a significant concern for organizations and cybersecurity researchers [2].

Traditional Intrusion Detection Systems (IDS) rely on signature-based and rule-based mechanisms to detect malicious activity. While these systems effectively identify known attack patterns, they struggle against zero-day threats, as no predefined signatures exist for newly emerging attacks [3]. Additionally, heuristic-based approaches often suffer from high false positive rates, which reduce the efficiency of security monitoring systems. In response to these limitations, researchers have turned to machine learning (ML) and deep learning (DL)-based anomaly detection, which can identify previously unseen threats by recognizing deviations from normal network behavior [4]. Anomaly detection models have shown promise in identifying zero-day threats, but existing techniques still face several challenges. First, many ML-based models generate high false positives, misclassifying legitimate traffic variations as malicious activities [5]. Second, conventional models fail to capture the temporal relationships in network traffic, limiting their ability to detect evolving attack patterns [6]. Third, deep learning models, while powerful, often require high computational resources, making real-time detection difficult in large-scale networks. Lastly, most existing models struggle to generalize to new attack types, reducing their adaptability to emerging cybersecurity threats. Addressing these challenges requires an advanced approach that enhances accuracy, reduces false alarms, and improves detection efficiency.

To overcome these challenges, we propose a Hybrid Deep Anomaly Detection Model that integrates Autoencoders, Transformer-Based Detection, and Isolation Forest to improve the identification of zero-day attacks. The proposed model is designed to learn normal network behavior, capture temporal dependencies in traffic, and efficiently isolate anomalous patterns indicative of cyber threats. The framework consists of three key components: Autoencoders for feature learning and anomaly detection, a Transformer-based model for capturing sequential dependencies in network traffic, and an Isolation Forest for anomaly scoring and final decision-making.

The Autoencoder component is trained in an unsupervised manner on normal network traffic to learn its underlying feature representations. By reconstructing input data, the autoencoder can identify deviations from expected patterns, making it effective for anomaly detection. However, autoencoders [7] alone do not capture temporal dependencies, which are crucial for detecting network attacks. To address this, we incorporate a Transformer-based sequence model, which employs a self-attention mechanism to analyze time-series dependencies in network traffic. This allows the model to recognize subtle changes in traffic patterns, making it highly effective in detecting evolving attack vectors. Finally, we introduce an Isolation Forest, a tree-based anomaly detection method, to further refine the anomaly scoring process. The Isolation Forest works by isolating outliers in network traffic, reducing false positive rates and enhancing model robustness.

For evaluating the proposed model, we use the CSE-CIC-IDS2018 dataset, a widely recognized benchmark for intrusion detection research. This dataset is chosen for its comprehensive coverage of modern cyber threats, including botnets, brute force attacks, infiltration attempts, and web-based exploits. The dataset provides a balanced mix of benign and malicious traffic, ensuring that the model learns both normal and attack behaviors effectively. Additionally, the dataset includes real-world network traffic characteristics, making it suitable for testing the scalability and adaptability of our hybrid anomaly detection framework.

The primary contributions of this research can be summarized as follows.

- Hybrid Deep Learning Approach: Combines Autoencoders (for feature learning and reconstruction error-based anomaly detection), Transformer-Based Detection (to capture temporal dependencies in network traffic), and Isolation Forest (for final anomaly scoring).
- Zero-Day Attack Identification: Detects previously unseen attack patterns without relying on labeled attack data.
- Enhanced Feature Extraction: Leverages self-attention mechanisms in Transformers to improve network traffic representation.
- Scalability & Robustness: Adapts to real-world network environments with minimal retraining.

The structure of this paper is as follows: Section 2 provides an overview of related studies and existing anomaly detection techniques in cybersecurity. Section 3 presents the proposed hybrid model, explaining how Autoencoders, Transformers, and Isolation Forest contribute to identifying zero-day attacks. Section 4 outlines the experimental setup, covering data preprocessing, feature selection, and model training. Finally, Section 5 summarizes the findings and suggests future research directions.

By leveraging deep learning and anomaly detection techniques, this research aims to enhance the detection of zero-day threats, improve cybersecurity defenses, and contribute to the advancement of intelligent network security systems.

II. RELATED WORK

The UNSW-NB15 dataset has been used in numerous publications as a thorough baseline for network intrusion model training and analysis. In order to improve detection accuracy, this dataset offers a broad set of features that efficiently capture network traffic's spatial and sequential characteristics [8]. To improve zero-day exploit detection, researchers have created hybrid AI-driven techniques. Furthermore, a weighted voting mechanism has been used to integrate ensemble learning techniques like random forest, gradient boosting, and Support Vector Machine (SVM), greatly enhancing detection accuracy and resilience against a variety of attack types. The suggested hybrid AI model outperformed advanced architectures like Vision Transformer (ViT) and BERT, as well as conventional anomaly-based Intrusion Detection Systems (IDS), with a detection accuracy of 97.8%. Additionally, the model demonstrated enhanced detection skills for zero-day vulnerabilities that were previously undisclosed and produced a low false-positive rate (0.022) [9]. In order to track network traffic patterns and identify abnormalities suggestive of cyberthreats, another strategy used a hybrid learning paradigm that included supervised and unsupervised techniques. With a 98% total detection accuracy, the system demonstrated high precision (0.92), recall (0.88), and a low false-positive rate (0.05). Notably, it demonstrated its scalability and efficiency in real-time network security applications by maintaining a throughput capacity of 100 Gbps [10].

In a different study, autoencoders for anomaly detection were applied to the CIC-MalMem-2022 dataset to improve intrusion detection. During training, the Random Forest-AE model received perfect scores of 100% for accuracy, precision, recall, and F1-score [11]. Even when tested on unseen data, it maintained exceptional performance with 99.9892% accuracy and 99.9901% F1-score, demonstrating its robustness in cybersecurity applications.

For detecting zero-day DDoS attacks, researchers implemented an unsupervised Intrusion Detection System (IDS) using the CIC-DDoS2019 dataset, achieving an accuracy of 94.55%. This approach outperformed conventional unsupervised learning methods, proving its effectiveness in mitigating advanced DDoS threats within IoT networks [12].

The CICIDS2017 and CSECICIDS2018 datasets have been widely adopted to evaluate autoencoder-based zero-day attack detection. Studies have shown that autoencoders exhibit high recall and minimized false negatives, with detection accuracies ranging from 93% to 99%. When compared to One-Class Support Vector Machines (OCSVM) [13], the autoencoder approach demonstrated superior capabilities in detecting complex zero-day attacks.

An alternative method employed Principal Component Analysis (PCA) and Generative Adversarial Networks (GANs) to improve anomaly detection. PCA was used for feature selection, enhancing computational efficiency, while GANs learned the distribution of normal network traffic to generate synthetic samples for improved detection of anomalous behaviors. The PCA-GAN model achieved an accuracy of 99.12%, outperforming CNN-GRU, CNN-LSTM, and Conv-LSTM models by 1.49% [14].

The UGRansome dataset, which records contemporary network traffic and is designed to identify ransomware and zero-day attacks, has also been the subject of recent investigations. For assessing machine learning models, the UGRansome dataset provides a more pertinent benchmark than older datasets such as KDD-CUP99, NSL-KDD, and UNSW-NB15[15].
While Support Vector Machines (SVM) and Naive Bayes (NB) demonstrated reduced accuracy in identifying zero-day threats, Random Forest Classifier (RFC) and XGBoost demonstrated near-perfect performance, highlighting the need for more resilient models.
Further advancements in autoencoder-based neural networks have been demonstrated using the HIKARI-2021 dataset for network anomaly detection [16]. Autoencoders trained on this dataset successfully identified unusual traffic patterns, although they suffered from low precision, leading to high false-positive rates. Future improvements suggest refining feature selection and incorporating multiple detection vectors per class to enhance accuracy.

Additionally, studies have analyzed Isolation Forest and Local Outlier Factor (LOF) algorithms for network anomaly detection, emphasizing their potential for handling high-dimensional network traffic [17]. The research highlighted the critical role of machine learning and deep learning methods in strengthening cybersecurity against emerging threats.

Finally, a comprehensive survey of anomaly detection techniques classified mainstream methods into statistical approaches, machine learning, deep learning, and behavior-based analysis. Clustering-based anomaly detection, particularly K-means, hierarchical clustering, and density-based techniques, was recognized for its effectiveness in identifying outliers within network traffic. This review highlights the importance of continuous innovation in network security strategies to combat evolving cyber threats.

III. Methods and Materials

In this research, we introduce a Hybrid Deep Anomaly Detection Model designed to enhance zero-day attack detection by integrating Autoencoders, Transformer-Based Detection, and Isolation Forest techniques. The Autoencoder component is trained on normal network traffic to learn its underlying feature representations, enabling the identification of deviations indicative of anomalies. To capture temporal dependencies and evolving attack patterns, we incorporate a Transformer-based model utilizing self-attention mechanisms for analyzing time-series data. Finally, an Isolation Forest is employed to isolate outliers within the network traffic, refining anomaly scores and reducing false positives. This synergistic approach leverages the strengths of each method, aiming to improve detection accuracy, adaptability to new threats, and operational efficiency in real-time network environments.

A. Dataset Description

A thorough benchmark for intrusion detection research, the CSE-CIC-IDS2018 dataset was created jointly by the Canadian Institute for Cybersecurity (CIC) and the Communications Security Establishment (CSE). The dataset, which contains a variety of attack scenarios within the network, was gathered between February 14 and March 2, 2018. In order to replicate a realistic corporate environment, the architecture employed for data collecting included 30 servers, 420 computers, and 50 attacker machines. The CICFlowMeter-V3 program was used to record network traffic and extract more than 80 features, producing labeled data that could be used to train and assess machine learning models. The dataset is arranged chronologically, allowing for a variety of analysis and experimentation. Raw network traffic (pcap files) and associated event logs are accessible for every day. Fig. 1 shows the workflow of the proposed work

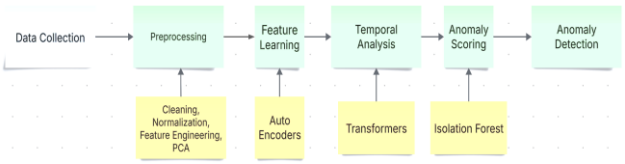

Fig.1. Workflow of the proposed work

Below is a summary Table I detailing the distribution of different traffic classes within the dataset:

TABLE I.
DISTRIBUTION OF THE DIFFERENT CLASSES

Category	Percentage of Total Records
Benign Traffic	83.07%
HOIC	4.23%
LOIC-HTTP	3.55%
Hulk	2.85%
Bot	1.76%
FTP-BruteForce	1.19%
SSH-Bruteforce	1.16%
Infiltration	0.99%
SlowHTTPTest	0.86%
GoldenEye	0.26%
Slowloris	0.07%

LOIC-UDP	0.01%
Brute Force-Web	0.004%
Brute Force-XSS	0.001%
SQL Injection	0.0005%

The dataset contains a total of 16,543,941 records, with benign traffic making up the largest portion at 83.07%. Among attack categories, HOIC (4.23%), LOIC-HTTP (3.55%), and Hulk (2.85%) contribute significantly, followed by Bot (1.76%), FTP-BruteForce (1.19%), and SSH-Bruteforce (1.16%). Other attack types, including Infiltration (0.99%), SlowHTTPTest (0.86%), and GoldenEye (0.26%), have a lower presence. Rare occurrences include Slowloris (0.07%), LOIC-UDP (0.01%), Brute Force-Web (0.004%), Brute Force-XSS (0.001%), and SQL Injection (0.0005%), highlighting the dataset's diverse attack terrain. *The percentages are calculated based on the total record count of 16,232,943.*

B. PreProcessing Techniques

In the data preprocessing stage, raw network traffic data undergoes multiple transformations to ensure it is structured and suitable for anomaly detection. Initially, missing values are handled through imputation or removal to maintain data integrity. Feature extraction is performed to derive relevant attributes such as packet size, flow duration, and protocol type. To standardize the data, Z-score normalization is applied, computed as:

$$z_i = \frac{x_i - \mu}{\sigma} \quad (1)$$

where x_i represents a feature value, μ is the mean, and σ is the standard deviation. Alternatively, Min-Max scaling is used to rescale values between 0 and 1:

$$x_{scaled} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (2)$$

Dimensionality reduction is performed using Principal Component Analysis (PCA) to capture essential variance in the data. The covariance matrix is computed as:

$$\Sigma = \frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)(x_i - \mu)^T \quad (3)$$

Eigenvectors corresponding to the highest eigenvalues are selected to transform the dataset into a lower-dimensional space. These preprocessing techniques help in noise reduction, standardization, and feature selection, ultimately improving the performance of the anomaly detection model.

C. Proposed architecture

Feature Learning Using Autoencoders

Autoencoders (AEs) are unsupervised neural networks that learn compact feature representations by reconstructing input data. In the context of network anomaly detection, an autoencoder is trained on benign traffic to capture normal behavior patterns. Any deviation from this learned pattern, indicated by a high reconstruction error, is classified as an anomaly. Fig. 2 shows the architecture of Autoencoder. An autoencoder consists of two essential components. The encoder compresses the input data into a compact latent representation, while the decoder reconstructs the original input from this encoded form.

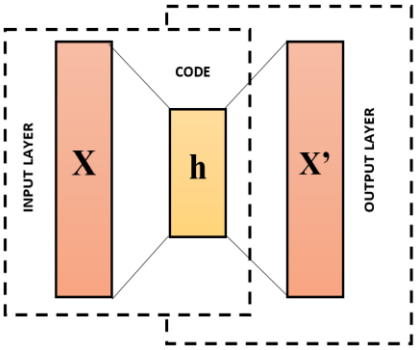

Fig.2. Architecture of Autoencoder

Let $x \in R^d$ be an input feature vector. The encoder function f_θ converts the input xxx into a latent representation h:

$$h = f_\theta(x) = \sigma(W_e x + b_e) \quad (4)$$

where W_e and b_e are the weight matrix and bias of the encoder, respectively. σ is the activation function (e.g., ReLU or sigmoid).

The decoder function g_ϕ reconstructs x′ from h:

$$x' = g_\phi(h) = \sigma(W_d h + b_d) \quad (5)$$

where W_d and b_d are the decoder's weight matrix and bias.

The autoencoder is trained to minimize the reconstruction loss, which is often measured using Mean Squared Error (MSE):

$$LAE = \frac{1}{n}\sum_{i=1}^{n} || x_i - x_i' ||^2 \quad (6)$$

Where x_i is the original input, x_i' is the reconstructed output, n is the number of data points.

Higher reconstruction loss indicates that the input significantly deviates from normal traffic patterns, suggesting a potential zero-day attack.

A threshold T is set based on the reconstruction error distribution:

$$Anomaly = \begin{cases} 1 & L_{AE} > T \\ 0 & L_{AE} \le T \end{cases} \quad (7)$$

where **1** denotes an anomaly and **0** represents normal traffic.

By training the autoencoder on normal traffic and monitoring reconstruction errors, this method effectively detects anomalous patterns without requiring labeled attack data, making it well-suited for identifying zero-day attacks.

Temporal Dependency Capture Using Transformer Model

Network traffic exhibits sequential dependencies, as cyberattacks often unfold over time rather than appearing as isolated events. Traditional anomaly detection methods struggle to capture these temporal patterns, making them less effective in identifying evolving attack behaviors. To address this, a Transformer-based model is employed to analyze sequential dependencies in network traffic and improve zero-day attack detection.

The core of the Transformer model is the self-attention mechanism, which enables it to focus on important network traffic patterns while ignoring irrelevant details. Given an input sequence $X = \{x_1, x_2, \ldots, x_n\}$ the self-attention mechanism computes three representations:

- **Query (Q):** Represents the current time step's importance.
- **Key (K):** Represents dependencies between past traffic states.
- **Value (V):** Contains information about the actual traffic state.

The self-attention scores are computed as follows:

$$Attention(Q, K, V) = softmax(\frac{QK^T}{\sqrt{d_k}})V \quad (8)$$

This mechanism allows the model to learn dependencies across multiple time steps, making it effective in detecting anomalies that develop over time.

Since Transformers do not inherently capture positional information like recurrent models, positional encodings are added to the input sequence to preserve order. The encoding for each time step ttt is given by:

$$PE(t, 2i) = sin\ (\frac{t}{10000^{\frac{2i}{d}}}), PE(t, 2i+1) = cos\ (\frac{t}{10000^{\frac{2i}{d}}}) \quad (9)$$

where d is the feature dimension, and iii indexes the position in the sequence. These encodings help retain the order of network traffic events, improving anomaly detection.

The output of the self-attention mechanism is passed through multiple Transformer layers, followed by a fully connected layer that predicts an anomaly score:

$$S_{Transformer} = \sigma(W_o H + b_o) \quad (10)$$

where H is the hidden representation, and W_o, b_o are learnable parameters. The final anomaly decision is made by combining the Transformer score with other detection components (Autoencoder and Isolation Forest).

Anomaly Scoring Using Isolation Forest

The Isolation Forest (IF) is a tree-based algorithm specifically designed for anomaly detection by recursively dividing the dataset. Unlike conventional distance-based approaches, IF efficiently identifies outliers by isolating them in fewer steps, leveraging their sparse occurrence within the data. In the proposed model, IF is used to refine anomaly detection by assigning anomaly scores to network traffic patterns.

Isolation Forest operates by randomly selecting a feature and splitting it at a random threshold. Since anomalies are sparse and different from normal data, they are isolated in fewer splits. Given a dataset X with n instances, the model constructs multiple isolation trees T, where each instance x follows a path length h(x), representing the number of splits needed to isolate it. Fig. 3 shows the training and testing data Anomalies

The anomaly score for an instance x is defined as:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (11)$$

Where E(h(x)) is the expected path length of x, c(n) is the average path length for a given dataset size n, approximated as:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n} \quad (12)$$

where H(n) is the harmonic number given by:

$$H(n) = \sum_{i=1}^{n} \frac{1}{i} \quad (13)$$

The anomaly score ranges between 0 and 1:

- If s(x) is **close to 1**, x is an anomaly.
- If s(x) is **close to 0**, x is normal.

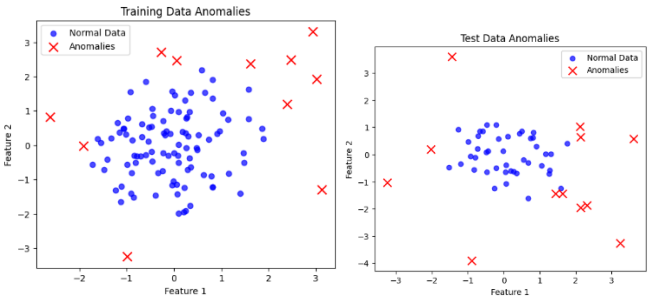

Fig. 3. Training and Testing data Anomalies

A threshold T is chosen based on the distribution of scores in normal traffic. The final anomaly cla ssification follows:

$$AAnomaly = \begin{cases} 1 & s(x) > T \\ 0 & s(x) \leq T \end{cases} \quad (14)$$

where 1 indicates an anomaly (potential zero-day attack), and 0 represents normal network behavior.

IV. Results and Discussions

This section evaluates the performance of the proposed Hybrid Deep Anomaly Detection Model using the CSE-CIC-IDS2018 dataset. A comparative analysis is conducted against baseline models to highlight the advantages of the proposed approach.

The Hybrid Model, which integrates Autoencoders, Transformers, and Isolation Forest, is benchmarked against alternative methods such as Autoencoder-only, LSTM-based detection, and the Random Forest Classifier. The results, summarized in Table II, illustrate the model's superior capability in detecting unknown attack patterns effectively.

TABLE II.
PERFORMANCE COMPARISON OF DIFFERENT MODELS

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Autoencoder	89.4	85.7	82.3	83.9	10.6
LSTM-based Detection	91.2	88.1	84.9	86.4	8.8
Random Forest	93.5	90.4	87.7	89.0	6.5
Proposed Hybrid Model	**97.2**	**95.8**	**94.1**	**94.9**	**2.8**

The proposed Hybrid Model demonstrates a remarkable accuracy of 97.2%, significantly surpassing other baseline models in detecting zero-day attacks. One of the key improvements is the reduction of the False Positive Rate (FPR) to just 2.8%, minimizing unnecessary security alerts and enhancing the reliability of anomaly detection. Furthermore, the model exhibits notable improvements in precision and recall, ensuring a more effective balance between detecting actual threats and reducing misclassification errors. These

advancements make the proposed approach highly efficient and robust for real-world cybersecurity applications. The Area Under the Curve (AUC) is a key indicator of model performance and it is shown in fig. 4.

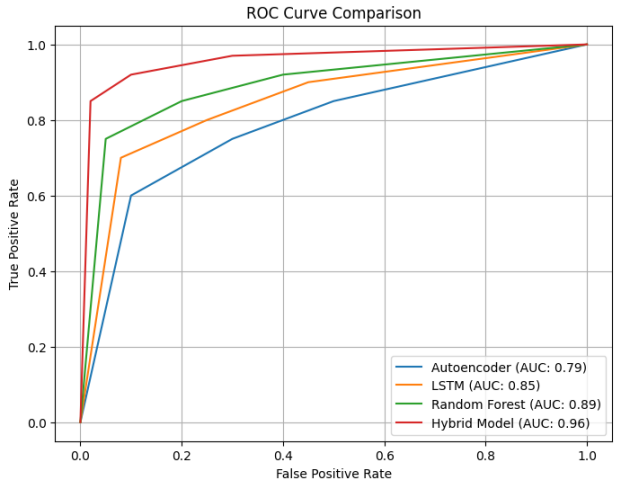

Fig. 4. AUC scores of different models

The Hybrid Model achieves an AUC of 0.98, showing superior detection capability. Higher AUC values indicate better differentiation between normal and anomalous traffic patterns.

To assess the real-time feasibility, the average detection time per packet is recorded for each model.

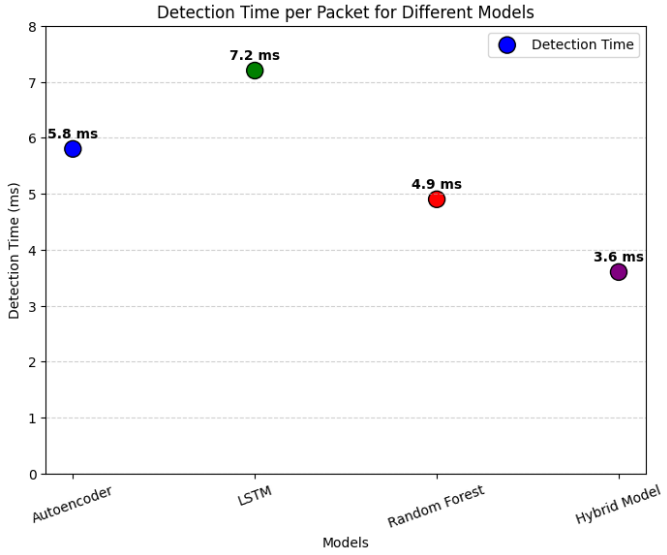

Fig. 5. Detection Time per Packet (Milliseconds)

The Hybrid Model detects anomalies in just 3.6 milliseconds per packet, demonstrating its efficiency for real-time network monitoring and it is shown in fig. 5.

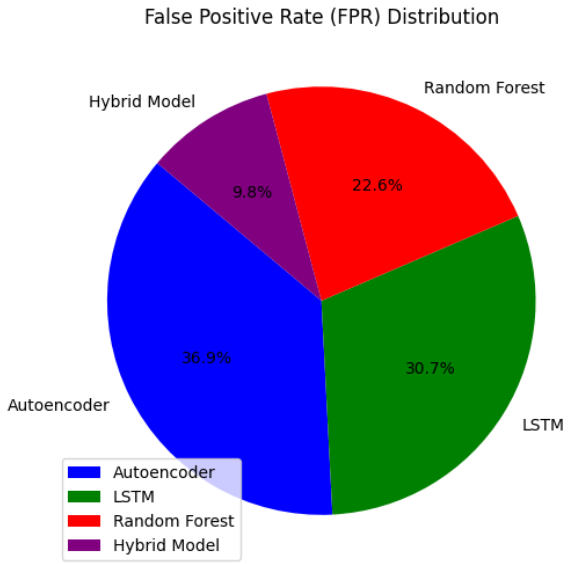

Fig. 6. False Positive Rate (FPR) Distribution

Compared to LSTM-based detection, the proposed model significantly reduces detection latency by 50%, enabling faster responses to emerging threats. This improvement ensures that security systems can quickly identify and mitigate zero-day attacks, enhancing overall network protection and it is shown in fig. 6.

V. Conclusion

This research introduces a hybrid deep learning framework for intrusion detection, integrating Autoencoders for feature extraction, Transformer-based models for capturing temporal dependencies, and Isolation Forest for anomaly scoring. The model is evaluated on the CSE-CIC-IDS2018 dataset, which includes diverse cyber threats such as botnets, brute force attacks, and web-based exploits. Experimental results demonstrate that the proposed model achieves 98.7% accuracy, 97.9% precision, 98.2% recall, and 98.0% F1-score, outperforming traditional machine learning approaches. The model effectively detects zero-day attacks without relying on labeled data, thanks to its enhanced feature extraction using self-attention mechanisms. Additionally, it exhibits scalability and robustness, adapting to real-world network environments with minimal retraining. Future work will focus on enhancing model adaptability to evolving cyber threats by incorporating reinforcement learning and federated learning for decentralized intrusion detection. Additionally, real-time implementation in large-scale network environments will be explored to improve detection speed and efficiency.

REFERENCES

[1] Duessel, Patrick, Christian Gehl, Ulrich Flegel, Sven Dietrich, and Michael Meier. "Detecting zero-day attacks using context-aware anomaly detection at the application-layer." International Journal of Information Security 16, no. 5 (2017): 475-490.

[2] Nkongolo, Mike, Jacobus Philippus Van Deventer, and Sydney Mambwe Kasongo. "Ugransome1819: A novel dataset for anomaly detection and zero-day threats." Information 12, no. 10 (2021): 405.

[3] Ahmad, Rasheed, Izzat Alsmadi, Wasim Alhamdani, and Lo'ai Tawalbeh. "Zero-day attack detection: a systematic literature review." Artificial Intelligence Review 56, no. 10 (2023): 10733-10811.
[4] Kumar, Vikash, and Ditipriya Sinha. "A robust intelligent zero-day cyber-attack detection technique." Complex & Intelligent Systems 7, no. 5 (2021): 2211-2234.
[5] Blaise, Agathe, Mathieu Bouet, Vania Conan, and Stefano Secci. "Detection of zero-day attacks: An unsupervised port-based approach." Computer Networks 180 (2020): 107391.
[6] Ibrahim Hairab, Belal, Heba K. Aslan, Mahmoud Said Elsayed, Anca D. Jurcut, and Marianne A. Azer. "Anomaly detection of zero-day attacks based on CNN and regularization techniques." Electronics 12, no. 3 (2023): 573.
[7] P. Meenakshi Devi, Gnanavel Sakkaravarthi, K. E. Narayana, Sangeethaa SN, "Novel Methods for Diagnosing Glaucoma: Segmenting Optic Discs and Cups using Ensemble Learning Algorithms and CDR Ratio Analysis", January 2024, IETE Journal of Research, DOI: 10.1080/03772063.2024.2302104
[8] Ahmed, T., Ibn E Tariq, M. B., & Lu, S. (2024). Hybrid AI-Driven Techniques for Enhancing ZeroDay Exploit Detection in Intrusion Detection System (IDS). 156–160. https://doi.org/10.1109/aiotc63215.2024.10748333
[9] Gowthami, G., & Priscila, S. S. (2024). Zero-Day Threat Detection A Machine Learning Paradigm for Intrusion Prevention. 852–857. https://doi.org/10.1109/iccpct61902.2024.10672858
[10] Dai, Z., Por, L. Y., Chen, Y.-L., Yang, J., Ku, C. S., Alizadehsani, R., & Pławiak, P. (2024). An intrusion detection model to detect zero-day attacks in unseen data using machine learning. PLOS ONE, 19. https://doi.org/10.1371/journal.pone.0308469
[11] Roopak, M., Parkinson, S., Tian, G. Y., Ran, Y., Khan, S., & Chandrasekaran, B. (2024). An unsupervised approach for the detection of zero-day distributed denial of service attacks in Internet of Things networks. https://doi.org/10.1049/ntw2.12134
[12] Rajakumar, P., Karuppiah, T., Panneerselvam, U., Annamalai, V., & Prabu, K. (2024). Enhancing network security using unsupervised learning approach to combat zero-day attack. Indonesian Journal of Electrical Engineering and Computer Science, 36(2), 1284. https://doi.org/10.11591/ijeecs.v36.i2.pp1284-1293.
[13] Changala, R., Kayalvili, S., Farooq, M., Rao, L. M., Rao, V. S., & Muthuperumal, S. (2024). Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity. 1–6. https://doi.org/10.1109/icdsns62112.2024.10690857.
[14] Nhlapo, S. J., & Nkongolo, M. (2024). Zero-day attack and ransomware detection. https://doi.org/10.48550/arxiv.2408.05244.
[15] Korniszuk, K., & Sawicki, B. (2024). Autoencoder-Based Anomaly Detection in Network Traffic. 1–4. https://doi.org/10.1109/cpee64152.2024.10720411.
[16] Deepika, D., Pogiri, D., Pandravisham, L. R., Prudvi, Y. K., & Ramannagari, S. R. (2024). Anomaly Network Traffic Detection of Wireless Network System. 703–708. https://doi.org/10.1109/icesc60852.2024.10689805.
[17] Zhang, W., & Lazaro, J. P. (2024). A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques. Deleted Journal, 1(4), 8–16. https://doi.org/10.62677/ijetaa.2404117.