Proceedings of the 6th International Conference on Inventive Research in Computing Applications (ICIRCA-2025)
IEEE Xplore Part Number: CFP25N67-ART; ISBN: 979-8-3315-2142-4

Self-Supervised Anomaly Detection for DoS Attacks using Autoencoders with Attention Mechanism and Real-Time Detection

Jayshnav S
Department of Computing Technologies
SRM Institute of
Science and Technology,
Chennai, India
js4264@srmist.edu.in

Archana Mahendran
Department of Computing Technologies
SRM Institute of
Science and Technology,
Chennai, India
am1594@srmist.edu.in

Jeyasekar A
Department of Computing Technologies
SRM Institute of
Science and Technology,
Chennai, India
jeyaseka@srmist.edu.in

2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA) | 979-8-3315-2142-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICIRCA65293.2025.11089924

***Abstract*— Denial of Service (DoS) attack is an attack making the computational resources unavailable or unpairing network geographically or creating operational downtime. It results in service disruptions, reputational damages, and financial losses. There are many methods for detecting the DoS attack which uses flow-based, packet-based, behavioral-based and signature-based analysis. In recent years, supervised and unsupervised learning methods are used to detect the DoS attack. But, in this paper, an attention-based autoencoder with self-supervised learning for DoS attack detection is proposed. Furthermore, the proposed method is integrated with FAST API which makes it a real-time detection system and provides a quick inference for live network traffic analysis. Since the proposed method uses self-supervised learning, it learns only from normal traffic data thereby deviation from normal traffic is considered as DoS attack. A reconstruction loss threshold set at the 95th percentile is used to find any changes from this learned distribution that could be signs of attacks. To train and test the proposed method, the NSL-KDD dataset is used. The performance of the proposed method is measured using F1-score, ROC-AUC, Recall, Accuracy, Precision and Confusion matrix analysis. A high reconstruction loss value essentially suggests abnormal behavior, enabling effective anomaly detection. The experimental results prove that the proposed architecture provides better performance in detecting the DoS attack in the regular traffic with 97.60% accuracy.**

Keywords— DoS Attack Detection, Self-Supervised Learning, Autoencoder, Attention Mechanism, Anomaly Detection, Reconstruction Loss, FAST API

I. INTRODUCTION

Denial-of-service (DoS) attacks are cyber threats intended to flood a network, server, or service with illicit traffic, consequently impairing victim from network or creating operational downtime or resource unavailable. Such attacks may lead to service interruptions, decreased performance, and severe financial or reputational damage [1]. DoS attacks have grown more common and difficult to identify as networks have become more complex. Sustained DoS attacks in severe conditions could disrupt essential online services, affecting sectors including government services, banking, and healthcare. Volume-based (e.g., UDP floods) [2], protocol-based (e.g., SYN floods) [2], and application-layer attacks (e.g., HTTP floods) [3] are the difference types of DoS attacks. Each type uses different methods to generate the illicit traffic. Therefore, the detecting the DoS attack is a challenging one. Mass data flooding the target from volume-based attacks utilizes bandwidth severely. While application-layer attacks target specific application's functions and are harder to detect, protocol-based attacks use the limitations in network protocols to consume resources. Conventional rule-based systems frequently struggle to identify novel or evolving attack patterns. Conversely, supervised learning techniques rely on balanced and labelled data for training, which lacks in generalizing the unseen attack patterns [4]. Therefore, identifying and mitigating DoS attacks is crucial for preserving network security.

Hence in this paper, self-supervised learning is used for DoS attack detection which learns from normal traffic data and detects the anomalies by identifying the deviations from normal behavior after the training phase. This approach is particularly useful in detecting the new attack variants. In contrast to supervised learning, Self-Supervised Learning enhances scalability and adaptability in dynamic network environments by eliminating the manual labelling of attack samples [5]. Furthermore, an attention-based autoencoder trained on the NSL-KDD dataset using self-supervised learning is employed. Normal data is used for training to capture the underlying distribution of standard behavior. The input traffic that deviates from this distribution is considered as anomalies or DoS attack. FastAPI is made use of to facilitate the real-time monitoring and attack mitigation. The proposed method enhances detection accuracy and adapts to fluctuations in network environments. Robust real-time detection ensures proactive defense against DoS attacks, thereby enhancing cybersecurity resilience and reducing downtime [6].

The remaining portion of the paper is structured as follows: Section II reviews the Dos attack detection system using different ML techniques. Section III describes the proposed method which used the self-supervised learning with attention-based autoencoder, FastAPI. Section IV analyze the evaluation of the proposed system and eventually the research work is concluded in the Section V.

II. LITERATURE SURVEY

Numerous studies have investigated anomaly detection techniques in cybersecurity, particularly focusing on the identification of denial-of-service (DoS) attacks [7,8]. Conventional rule-based systems frequently struggle to adjust to emerging threats, prompting the implementation of machine learning models. Chandola et al. [9] presented fundamental anomaly detection methodologies, emphasizing the advantages of unsupervised frameworks for intrusion detection. Autoencoders became prominent, and Sakurada and Yairi [10] illustrated their efficacy in anomaly detection through reconstruction errors. Exploration of self-supervised learning methods utilizing

autoencoders has been conducted. Erfani et al. [11] effectively utilized deep autoencoders for intrusion detection, emphasizing on their adaptive capabilities. Vaswani et al. [12] showed that using autoencoders with attention mechanisms made tasks like finding anomalies much better [13,14]. It was implemented by introducing the powerful transformer architecture that focuses on attention. Existing research, mostly concentrates on stationary datasets and offline analysis, restricting their relevance in dynamic, real-time settings. By combining FastAPI with attention-based autoencoders for real-time DoS attack detection, the proposed system bridges this gap. DoS attacks specifically have been addressed through various machine learning frameworks using the NSL-KDD dataset which was produced by Tavallaee et al. [15], so enabling thorough benchmarking in research of DoS attack detection. By means of the NSL-KDD dataset, Yin et al. [16] conducted a thorough investigation of intrusion detection methods highlighting their effectiveness.

Moreover, classifiers such as Naive Bayes have been extensively studied; Panda and Patra [17] evaluated their system in anomaly detection over often used datasets. Belavagi and Muniyal [18] used and studied decision tree methods to find network intrusions that worked well. Logistic regression models have also showed effectiveness in intrusion detection scenarios, as discussed comprehensively by Buczak and Guven [19]. M. Ngueajio et al. [20] and Ahmad et al. [21] showed that machine learning can be used to analyze real-time network traffic. They deployed ensemble methods for practical intrusion detection scenarios. Zong et al. [22] and Malhotra et al. [23] discuss threshold methods for the effective classification of anomalies through percentile reconstruction loss. Goodfellow et al. [24] have advocated for the use of regularization techniques such as L1 and L2 to improve generalization. Although many studies have looked at conventional classifiers and thresholding techniques, they hardly fit changing network traffic patterns. This work dynamically alters detection thresholds using self-supervised learning and attention mechanisms to raise real-time accuracy.

Mirsky et al. [27] examined adaptive detection systems that employ autoencoder framework that is specifically designed for the detection of network anomalies. Al-Qatf et al. [28] conducted an analysis of deep learning methodologies in the field of cybersecurity, emphasizing their practical applicability for scalable and real-time anomaly detection [25,26]. While adaptive detection systems have advanced [29-31], few studies have looked at scalable, low-latency live-environment solutions. Using an attention-based autoencoder, this work rapidly detects and responds to anomalies.

Recent studies on DoS attack detection point up several research gaps. This is because they rely on labeled data and stationary detection rules. Due to which, traditional rule-based and supervised machine learning approaches sometimes find it difficult to change to new or developing attack patterns. Although unsupervised and self-supervised methods, such autoencoders, have shown potential for anomaly detection, most current research is limited to offline analysis on stationary datasets, so reducing their effectiveness in real-time, dynamic network environments. Few studies address scalable, low-latency solutions fit for live deployment; the use of attention mechanisms to improve feature discrimination is still under investigated. Targeting strong and adaptive DoS attack detection in modern network environments, this work aims to close these gaps by introducing an attention-based autoencoder with self-supervised learning and real-time detection capability.

III. PROPOSED SYSTEM

Fig 1 illustrates the overview of the proposed DoS attack detection using attention-based autoencoder and self-supervised learning. It consists of Data preprocessor, Attention-based encoder mechanism, Reconstruction score calculator and real time attack detector.

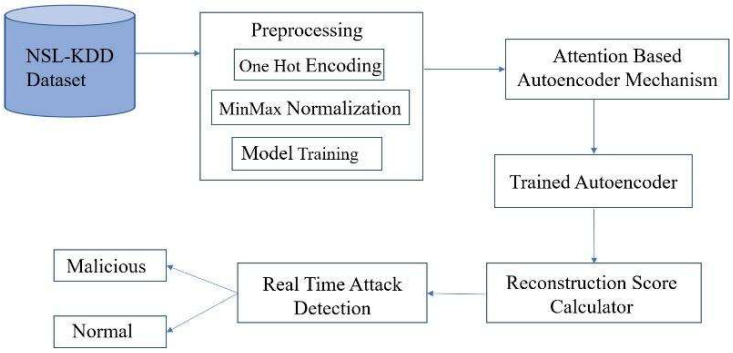

Figure 1: Overview of proposed system

A. Data Preprocessor

NSL-KDD dataset from Mireu-Lab/NSL-KDD repository via Hugging Face dataset library is used in this paper. It consists of network connection records labelled as either "Normal" or various types of "Attack". The labels are refined into a binary classification as Normal traffic (0) and Assault traffic (1), thereby improving the anomaly detection. The dataset has 41 attributes that describe the connection, content, and traffic. The categorical attributes like service, protocol type, flag etc. in the dataset are converted into numerical format by one-hot encoding which facilitates the efficient model training. Subsequently, numerical characteristics are normalized using a MinMaxScaler to ensure consistency and stability in model inputs. Following the data preprocessing, the dataset is partitioned into training set (80%) and testing set (20%).

B. Autoencoder

Implementing the principle of self-supervised learning, the autoencoder [27,28] is exclusively trained using the records labelled as "Normal" from training dataset. Trained solely on normal traffic dataset, the model captures the underlying distribution of standard behavior. During inference, input traffic that deviate from this learned distribution yield high reconstruction errors, which can be used to flag anomalies.

The autoencoder finds the unusual network traffic without requiring labelled dataset. It helps us to detect the anomaly traffic of DoS attacker.

C. Attention-Based Autoencoder Mechanism

In the proposed system, the autoencoder is enhanced using an attention technique [12] which results in better performance in distinguishing the anomaly traffic from normal traffic. The attention mechanism enhances model performance by dynamically weighting input features based on their relevance. In this paper, a self-attention within the autoencoder is employed, where Q (Query) represents the encoded feature vector of a network traffic sample, asking which parts of itself are most important for reconstruction. K (Key) is also the same data, used to check how similar each part is to the others. Together, they help the model figure out which parts of the input are most important to look at when trying to understand or rebuild the traffic pattern. V (Value) contains the real information or feature content that, depending on the computed attention ratings from Q and K, is weighted and combined. The weights on the values are derived by first computing the dot products of the query with every key, then dividing each by $\sqrt{d_k}$ using a softmax function. The softmax function converts the similarity scores into a probability distribution, from which a weighted sum over the values is subsequently computed. This whole process produces an attention output, a reweighted form of the input focusing on the most crucial elements for the task of rebuilding regular network activity in the proposed model.

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (1)$$

where d_k is the key dimension. This allows the model to capture long-range dependencies and hierarchical feature relationships in network traffic data. By focusing on salient patterns, the attention-based autoencoder improves reconstruction of normal traffic, while anomaly traffic are detected via threshold reconstruction error.

D. Reconstruction Score Calculator

Mean Square Error (MSE) is the loss function which has been used to calculate the reconstruction score. After the empirical analysis by varying the reconstruction threshold from 50 to 95, it is observed that 95th percentile of reconstruction loss as the anomaly threshold to distinguish between normal and anomalous traffic, thereby balancing false positives and detection sensitivity. Samples surpassing this threshold are categorized as DoS attacks, whereas others are deemed normal, facilitating real-time anomaly detection.

$$MSE = \frac{1}{m}\sum_{j=1}^{m}\left(P_j - \hat{P}_j\right)^2 \quad (2)$$

Where m refers to the total number of data points, P_j denotes the observed values and $\hat{P}_j$ refers to the predicted values.

E. Real Time Attack Detection Method

Combining a FastAPI inference pipeline with the proposed attention-based autoencoder detects anomaly traffics in real-time network. Known for its fast execution and simple interface with machine learning models, FastAPI is a high-performance modern web framework for creating APIs with Python. It is perfect for providing the proposed anomaly detection pipeline in live network environments since it offers asynchronous request handling, thus enabling real-time inference.

IV. RESULTS AND DISCUSSIONS

The experiment was conducted on Google Colab using a Tesla T4 GPU-accelerated runtime backed by a Windows 11 system with 64-bit OS, x64 processor, 13th Gen Intel(R) Core (TM) with 16 GB installed RAM. The attention-based autoencoder in the proposed system is trained with a batch size of 32 for 100 epochs, employing the AdamW optimizer for adaptive learning rate modifications and weight.

To avert overfitting, training exclusively utilized normal traffic, thereby ensuring the model identified benign patterns instead of memorizing attacks. A 10% validation split ensured stability monitoring. Despite the absence of explicit dropout or early stopping, batch normalization, L1/L2 regularization, and self-attention enhanced generalization and noise resilience

Figure 2 is a graph that depicts the nature of training and validation loss over 50 epochs. In the initial stage, training loss declines sharply indicating fast convergence as the model learns to reconstruct normal data. Validation loss also follows a similar pattern but it still remains higher proving that that the model is generalizing well without overfitting. Stability of both losses confirms convergence at a lower error rate.

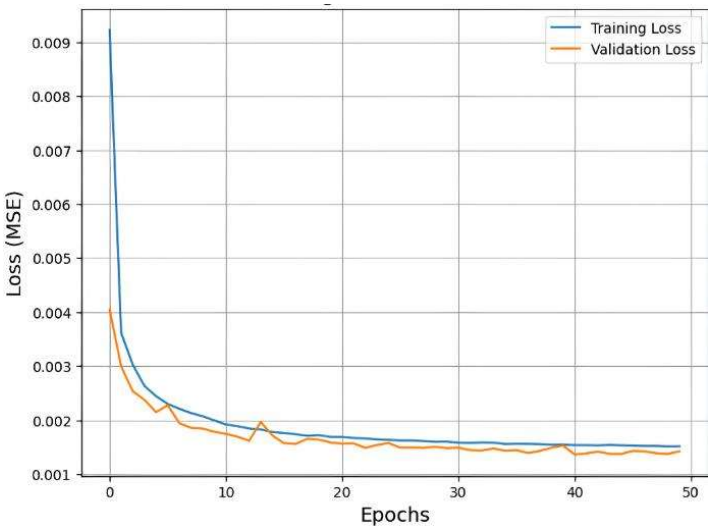

Figure 2: Training vs Validation Loss

Classification models are evaluated using confusion matrices, which show true positives (TP), true negatives (TN), false positives (FP), and false negatives. It evaluates model precision, recall, accuracy, and efficacy. This confusion matrix shows how well the model classifies normal and attack traffic. With 15,805 TN, 13,238 TP, 245 FP, and 945 FN, the model accurately distinguishes DoS attacks from normal traffic with a low incorrect classification rate. The obtained confusion matrix is shown in figure 3.

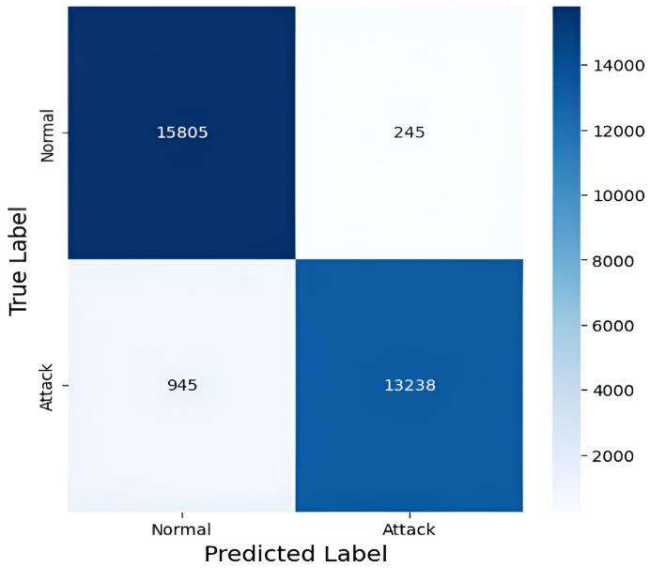

Figure 3: Confusion matrix

The ROC-AUC curve (Receiver Operating Characteristic - Area Under Curve) shows how well a classification model works by comparing the True Positive Rate to the False Positive Rate. Figure 4 presents a high AUC value (98.55), signifying that the model shows exceptional discriminatory ability between attack and normal traffic. The curve's significant increase implies few false positives and high sensitivity, making the model very accurate for identifying breaches.

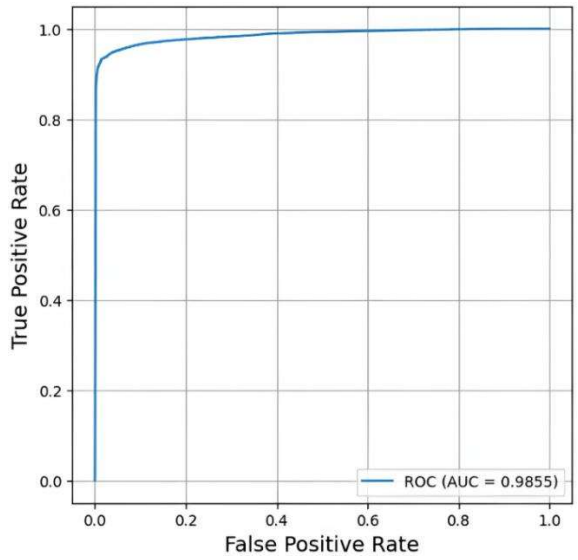

Figure 4: ROC – AUC curve

As the decision threshold is altered, the Precision-Recall curve in figure 5 shows how the model is able to maintain a balance between precision and recall. Initially, the precision remains high even as the recall increases. This indicates that the model successfully identifies attack traffic with a minimal number of false positives. On the other hand, as recall continues to increase, precision gradually declines. As demonstrated by this curve, the model is able to successfully detect a greater number of attacks while still preserving a high precision rate. This makes it a perfect fit for imbalanced datasets such as anomaly detection.

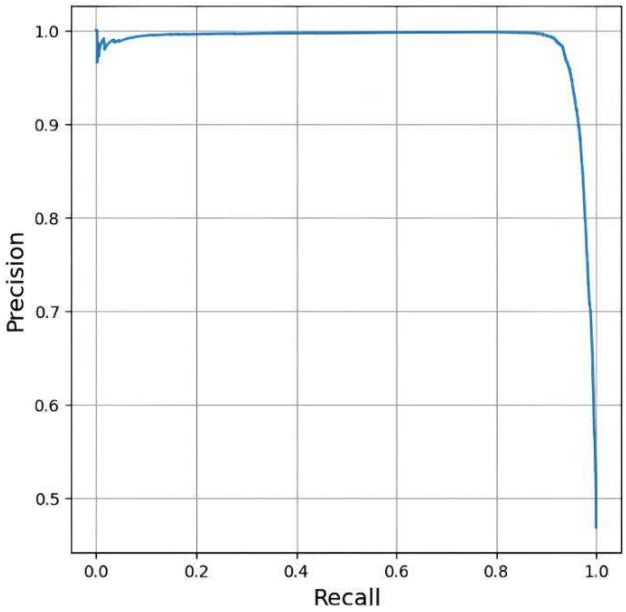

Figure 5: Precision-Recall curve

t-SNE (t-Distributed Stochastic Neighbour Embedding) is an approach which is implemented for performing dimensionality reduction. It enables viewing high-dimensional data in 2D or 3D. This method ensures that the local relationships between datapoints are preserved. Managing complex, high-dimensional datasets calls for this approach. The t-SNE plot shows the data points getting reduced to two dimensions. Blue points denote normal traffic, whereas the red points denote attack traffic. The plot depicts a distinct separation between the two classes, implying that the model has learned unique feature for normal and attack traffic very well. Though there is a distinct and significant separation, the centre region of the plot in figure 6 has some overlap between red and blue points. The overlap reveals possible false positives, and attack traffic is wrongly categorized as normal. Separating clusters shows effective feature learning for anomaly detection applications.

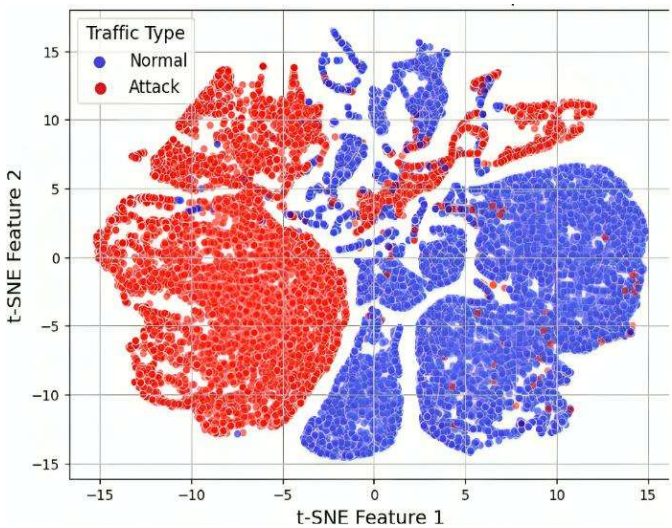

Figure 6: t-SNE Visualization of Latent Space

Table 1 shows the evaluation metrics of the model, with an accuracy of 97.60% and an F1-score of 95.70, so demonstrating strong classification performance. Strong discrimination between normal and attack traffic is confirmed by the high ROC-AUC (98.55%), thereby guaranteeing consistent anomaly detection.

Table 1. Model evaluation scores

Metrics	Obtained Value
Accuracy	97.60
Precision	98.18
F1 Score	95.70
Recall	93.34
ROC - AUC	98.55

Table 2 shows that the proposed model (97.60%), outperforms conventional classifiers including Naïve Bayes (84.32%) [32], XGBoost (88.13%) [33], Logistic Regression (88.86%) [34] and SVM (96.69%) [32]. Apart from traditional model developments, the approach's accuracy shows its reliability and strength in identifying DoS attacks. Combining attention mechanisms, L2 regularization, and real-time inference enhances its adaptability and accuracy even more—just fit for dynamic network environments.

Table 2. Comparison of various model performances

Model	Accuracy
Gaussian Naive Bayes	84.32
XGBoost	88.13
Logistic Regression	88.86
Decision Tree	95.83
SVM	96.69
Proposed Model	**97.60**

Table 3 shows how the accuracy consistently improves as the threshold value rises; from 76.30% at 55% threshold to an amazing 97.60% at 95% threshold. Concurrent with this, the false positive rate drops significantly from 7071 to just 245, thereby indicating the improved capacity of the model to accurately authorized traffic. Thus, the suggested model at 95% threshold finds an ideal balance between minimizing false positives and maximizing detection accuracy.

Table 3. Comparison of results for different threshold values

Threshold (%)	Accuracy (%)	True Positive	False Positive	True Negative	False Negative
55	76.30	14089	7071	979	94
65	82.16	14140	5351	10699	43
75	86.86	13997	3788	12262	186
85	91.72	13924	2244	13806	259
95 (Proposed Model)	**97.60**	**13238**	**245**	**13238**	**945**

The attention framework helps the model to focus on the most important and predominant features of the input data, thereby identifying significant trends for anomaly detection and improving the model. By means of dynamic weight distribution to salient features, the model raises its capacity to discriminate between normal and attack traffic. As table 4 shows, the inclusion of the attention mechanism clearly increases accuracy, precision, recall, and ROC-AUC. This outcome reveals that the inclusion of the attention mechanism is effective in improving the efficiency of the attack detection model compared to the model without attention.

Table 4. Comparison of results with and without Attention Mechanism

Comparison	Accuracy	Precision	F1 Score	Recall	ROC - AUC
Without Attention Mechanism	95.14	94.67	94.99	92.83	98.22
Attention Mechanism (Proposed Solution)	97.60	98.18	95.70	93.34	98.55

To summarize, in detection of DoS attacks, the proposed attention-based autoencoder with self-supervised learning outperformed conventional classifiers including Naïve Bayes, XGBoost, Logistic Regression, and SVM. With an accuracy of 97.60% and a ROC-AUC of 98.55%, the model was just trained on normal traffic and effectively found anomalies as attacks. The attention mechanism improved the emphasis on salient features, thereby reducing false positive incidence. Sensitivity and specificity were balanced using dynamic thresholding set at the 95th percentile. Real-time FastAPI execution, good results in t-SNE visualization and confusion matrix analysis of the model demonstrated its ability to adapt. This indicates the model's capability for dynamic configurations of networks.

V. CONCLUSION

This work proposed an attention-based autoencoder for real time network DoS attack detection. The proposed architecture is trained using NSL-KDD dataset. This model provides better performance than other classifiers like Gaussian naïve bayes, XGBoost, Logistic Regression SVM and Decision tree classifier with accuracy 97.60% and ROC-AUC 98.55% by using self-supervised learning and a coherent attention-based autoencoder mechanism. As shown in the confusion matrix, the 95th-percentile threshold strategy balanced false positives with sensitivity. Deployment through FastAPI facilitated scalable, low-latency inference, showcasing practical feasibility for dynamic network contexts. The model's interpretable attention weights and strong generalization underscore its appropriateness for detecting emerging threats. Future research may investigate adaptive thresholding and hybrid architectures to augment detection capabilities in extensive deployments. This method provides a dependable, automated resolution for contemporary intrusion detection systems.

VI. REFERENCES

[1] M. Raza, "Denial-of-Service Attacks in 2023: History, Techniques & Prevention," Splunk-Blogs, Feb. 01, 2023

[2] N. H. Syafiuddin, S. Mandala, and Niken Dwi Wahyu Cahyani, "Detection Syn Flood and UDP Lag Attacks Based on Machine Learning Using AdaBoost," pp. 36–41, Aug. 2023

[3] K. Singh, P. Singh, and K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," *Computers & Security*, vol. 65, pp. 344–372, Mar. 2017

[4] Ahmad Najar and S. Manohar Naik, "Applying Supervised Machine Learning Techniques to Detect DDoS Attacks," *2022 2nd Asian Conference on Innovation in Technology (ASIANCON)*, pp. 1–7, Aug. 2022

[5] M. Mozaffari, K. Doshi, and Y. Yilmaz, "Self-Supervised Learning for Online Anomaly Detection in High-Dimensional Data Streams," *Electronics*, vol. 12, no. 9, p. 1971, Apr. 2023

[6] E. Li, Z. Shang, O. Gungor, and T. Rosing, "SAFE: Self-Supervised Anomaly Detection Framework for Intrusion Detection," *arXiv preprint arXiv:2502.07119*, Feb. 2025

[7] Z. Li et al., "Denial of Service (DoS) Attack Detection: Performance Comparison of Supervised Machine Learning Algorithms," Aug. 2020

[8] S. Aktar and A. Yasin Nur, "Towards DDoS Attack Detection using Deep Learning Approach," Computers & Security, p. 103251, Apr. 2023

[9] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, Jul. 2009

[10] M. Sakurada and T. Yairi, "Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction," *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis - MLSDA'14*, 2014

[11] "High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning," *Pattern Recognition*, vol. 58, pp. 121–134, Oct. 2016

[12] Vaswani et al., "Attention is All you Need," *Neural Information Processing Systems*, 2017

[13] P. Li, Y. Pei, and J. Li, "A comprehensive survey on design and application of autoencoder in deep learning," Applied Soft Computing, vol. 138, p. 110176, May 2023

[14] M. Ganesh, A. Kumar, and V Pattabiraman, "Autoencoder Based Network Anomaly Detection," pp. 1–6, Dec. 2020

[15] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Jul. 2009

[16] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017

[17] M. Panda and M. Patra, "NETWORK INTRUSION DETECTION USING NAÏVE BAYES," *IJCSNS International Journal of Computer Science and Network Security*, vol. 7, 2007

[18] M. C. Belavagi and B. Muniyal, "Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection," *Procedia Computer Science*, vol. 89, pp. 117–123, 2016

[19] L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016

[20] M. Ngueajio, G. Washington, D. Rawat, and Y. Ngueabou, "Intrusion Detection Systems Using Support Vector Machines on the KDDCUP'99 and NSL-KDD Datasets. A Comprehensive Survey."

[21] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, pp. 1–29, Oct. 2020

[22] B. Zong et al., "Deep Autoencoding Gaussian Mixture Model for Unsupervised Anomaly Detection," *openreview.net*, Feb. 15, 2018

[23] P. Malhotra, A. Ramakrishnan, G. Anand, L. Vig, P. Agarwal, and G. R. Shroff, "LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection," Jul. 2016

[24] Goodfellow et al., *Deep learning*, MIT Press, Cambridge, MA, USA, 2016

[25] Javaid et al., "A deep learning approach for network intrusion detection system," *EAI Endorsed Trans. Security Saf.*, vol. 3, no. 9, pp. 1–15, 2016

[26] R. Chalapathy and S. Chawla, "Deep Learning for Anomaly Detection: A Survey," *arXiv:1901.03407 [cs, stat]*, Jan. 2019

[27] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," *arXiv:1802.09089 [cs]*, May 2018

[28] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018

[29] Sudha Anbalagan, Wajdi Alhakami, Mugundh Jambukeswaran Bhooma, Vijai Suria Marimuthu, K. Dev, and G. Raja, "Next-Gen Security: Enhanced DDoS Attack Detection for Autonomous Vehicles in 6G Networks," *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, pp. 1–5, Jun. 2024

[30] Kirubavathi G, S. Sivakumar, and S. Manickam, "Optimized Hybrid Approach for Anomaly Detection of DDoS and Network Attacks in IoMT Systems using Autoencoders and TabNet," pp. 1–7, Dec. 2024

[31] S. Agrawal et al., "Federated Learning for intrusion detection system: Concepts, challenges and future directions," *Computer Communications*, Sep. 2022

[32] Sarthak Rastogi, Archit Shrotriya, Mitul Kumar Singh, and R. V. Potukuchi, "An Analysis of Intrusion Detection Classification using Supervised Machine Learning Algorithms on NSL-KDD Dataset," *Journal of Computing Research and Innovation*, vol. 7, no. 1, pp. 118–130, Mar. 2022

[33] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," *Computer Communications*, Dec. 2022

[34] D. Vibhute, C. H. Patil, A. V. Mane, and K. V. Kale, "Towards Detection of Network Anomalies using Machine Learning Algorithms on the NSL-KDD Benchmark Datasets," *Procedia Computer Science*, vol. 233, pp. 960–969, Jan. 2024