Journal of Global Research in Electronics and Communication
Volume, 2 No. 06, June 2026
Available Online at: www.jgrec.info
RESEARCH PAPER

Design and Implementation of a Zero Trust Security Framework for Cloud-Based SaaS Applications

Dr. Neetu Sikarwar
Department of Electronice Engineering
Institute of Engineeeirng , Jiwaji University
Gwalior,India
Neetusik1@gmail.com

***Abstract*—Perimeter-based security solutions are becoming less and less effective due to the growing complexity of contemporary cyber threats and the collapse of old network boundaries. As a result, Zero Trust Architecture (ZTA) has become a revolutionary paradigm that redefines how cloud and hybrid IT infrastructures build, maintain, and revoke trust. This paper presents an intelligent Zero Trust Security Framework based on attention-based deep learning models to detect intrusions in real-time and dynamically enforce policies within SaaS applications. The framework combines the DNN + Attention and RNN + Attention models to continuously observe the network traffic and dynamically determine if the requests are legitimate or malicious and make ALLOW or DENY/QUARANTINE decisions. The CICIDS2017 dataset is used for experiment, followed by the preprocessing, feature analysis, data balancing using SMOTE and model training. Experimental results show that DNN + Attention model has the highest accuracy, F1 score and AUC-ROC of 97.00%, 92.75% and 99.63% respectively with less latency and faster prediction time compared to RNN + Attention model. The proposed framework is validated and demonstrated as effective in an intelligent intrusion detection, real-time threat containment, and secure SaaS application monitoring for current Zero Trust environments by comparing to existing approaches.**

Keywords—Zero Trust Security, SaaS Security, Intrusion Detection System, Threat Detection, Cloud Security, Machine Learning.

I. INTRODUCTION

Cloud platforms and SaaS apps are becoming more and more important to modern businesses in order to provide scalable and adaptable digital services. A contemporary cybersecurity paradigm known as "zero trust" makes the assumption that no human, system, or device, whether within or outside the network perimeter can be intrinsically trusted. It took the place of perimeter-based security approaches, which used firewalls and network borders to establish trust zones in the past [1][2]. The opposite is true with Zero Trust, which mandates constant authentication verification for all users and devices trying to access resources, irrespective of their location or authentication history [3][4]. A number of security mechanisms, including service-level agreements (SLAs), identity management and access controls, IDS, and application service management [5], have proven inadequate in preventing breaches in cloud-hosted government and corporate networks due to this explosive growth [6][7]. Cloud service customers (CSC) clearly implement these services on their networks according to their own requirements, choosing to do so based on their operating experiences and what is convenient for them. Top cloud network environments include Amazon Web Services, Microsoft AZURE, IBM Cloud, VMware, and Google Cloud [8][9].

Ransomware gangs, botnets, and advanced persistent threats (APT) continue to infiltrate cloud platforms and networks despite these intricate security solutions; the root cause of this problem is internal vulnerabilities and an inadequate security environment [10]. Furthermore, third-party apps on cloud networks might bring unexpected defects or even zero-day vulnerabilities [11], which attackers can use to access critical consumer data. Also, any user or even an APT within the network may inject third-party apps unless organizations check their sources.

AI has developed alongside cybersecurity as a cutting-edge technology for adaptive response systems, predictive analytics, and real-time threat detection [12][13][14]. Automating tasks like segmentation, identifying minute deviations or threats, and improving techniques to mitigate threats are all examples of how advanced AI features can be integrated into zero-trust effective systems to foster adaptive security [5]. Most significantly, it addresses issues with simple and rule-based security solutions and reaffirms the principles of Zero Trust.

A. Motivation and Contributions of the Study

As cloud computing and SaaS applications have come to the fore, so have the new and complex cybersecurity risks and threats that accompany them. Security models based on the perimeter are no longer cutting it in cloud environments that are constantly evolving, and that now demand a more intelligent security solution that can monitor continuously, adapt its authentication methods, and detects threats on the fly. Moreover, the existing intrusion detection techniques have problems such as not being easily scalable, high false alarm rate, and inability to handle complex network traffic patterns. These constraints led to the creation of attention-based DL approach for protected and efficient SaaS application protection. The following are the primary benefits of this study:

- A new Zero Trust Security Framework for SaaS is proposed based on attention-based deep learning models.
- The architectures of DNN + Attention and RNN + Attention are employed to realize intelligent intrusion detection with adaptive threat analysis.
- A dynamic policy enforcement mechanism is added to classify network traffic with ALLOW and DENY/QUARANTINE decisions.

- The models are robust and have good detection ability by using advanced pre-processing, feature selection and Class Balancing methods.
- Used a wide range of performance parameters to assess the framework's efficacy, including recall, accuracy, precision, latency, throughput, AUC-ROC, training time, and prediction time.

B. Structure of Paper

The rest of this paper is structured as follows: The relevant literature on ZeroTrust security is included in Section II. The suggested technique is explained in Section III. The findings of the experiment are shown in Section IV. The paper's conclusion and future study directions are outlined in Section V.

II. Literature Review

Researchers have increasingly focused on integrating Zero Trust architectures with ML and DL techniques to improve intrusion detection and adaptive security enforcement. S. Mishra et al. (2026) presents a Zero Trust enhanced intrusion detection framework that is built for low-latency inference and is well-suited for near-real-time IIoT monitoring. It incorporates features like deep learning anomaly detection, differential privacy, a lightweight ledger inspired by blockchain technology, and visualization of device trust states. A combined dataset was created by combining NSL-KDD, CICIDS-2017, and IoT-23. The combined dataset has 2,513,419 raw samples with 143 characteristics. Using SMOTE, 100,000 samples were balanced between Normal, DoS, Probe, R2L, and U2R classes. A total of 25 characteristics were narrowed down using mutual information-based feature selection. With an F1-score of 0.89 to 0.91 and an accuracy of 89 to 91%, the CNN-BiLSTM and Optimized MLP models were able to identify unusual attacks with a near-perfect performance ($F1 \approx 1.00$ for R2L/U2R) [15]. V. B Maniyat and A. Kumar B R et al. (2025) introduced an entropy-based drift detection mechanism and a continual learning module retrained with synthetic attack simulations and analyst feedback. Experimental evaluation across simulated attack scenarios demonstrates high accuracy (Fl-score of 95.0 %), robust ATT &CK coverage (89 %), and sub-second detection latency, confirming the framework's effectiveness for SOC integration [16].

M. Al-Zewairi et al. (2025) constructed a funnel-like hybrid approach that improves upon existing detection skills by combining two supervised and one unsupervised learning stage. On average, the suggested system achieves recall and accuracy levels between 88% and 95% when testing on four benchmark datasets, and it shows substantial gains when testing for unknown threats in terms of accuracy, recall, and mistake classification rates [17]. A. Jain et al. (2025) results of experimental assessments of the simulated environments show that Zero Trust Edge exceeds the conventional IIoT security models by enhancing the rate of detecting attacks by 26.4%, minimizing unnecessary energy consumption by 19.7%, and improving the explain ability of the decisions made by 31%. Zero Trust Edge creates a new paradigm addressing critical tradeoffs between resilience, transparency, and energy sustainability in future cyber- physical systems [18].

F. Guo et al. (2024) implemented a machine learning (ML) based network intrusion detection algorithm. The Intrusion Detection module has the ability to build models using various methods such as DL, SVM, and others. From 8:00 to 09:00, the real-time performance test results show an acc of 0.92, a false alarm rate of 0.05, and an Average Detection Time of 50 ms. From 09:00 to 10:00, the findings show an acc of 0.90, a false alarm rate of 0.06, and an average detection time of 55 ms [19]. M. Dhinakaran et al. (2024) analyze the efficacy of ML in protecting data stored in the cloud. This environment was used to test three distinct ML models. The RF model was used in Experiment 1, which yielded 95% acc, 0.92 prec, 0.96 rec, and 0.94 F1score. This demonstrates that the model successfully classifies security risks while maintaining a reasonable ratio of true positives to false positives [20]. H. Teymourlouei (2023) provide a RF-based ML strategy for assessing ZT compliance. All aspects of the system, including users, devices, apps, networks, data, and infrastructure, will be checked for compliance by the model. The model achieved a classification accuracy of above 95% for all six things, according to the findings [21].

A. Problem Statement and Gap Analysis

Although several existing studies have applied machine learning and Zero Trust architectures for intrusion detection and cloud security [22], many frameworks still face limitations related to high false alarm rates, limited real-time adaptability, computational complexity, and ineffective handling of dynamic SaaS traffic patterns. Most existing approaches focus either anomaly detection or policy enforcement alone and lack integration of intelligent attention-based deep learning model for adaptive Zero Trust decision making. Moreover, most of the traditional models are not efficient in terms of threat prioritization, scale of real-time monitoring and performance against sophisticated and evolving cyberattacks. Thus, the need for an intelligent and efficient Zero Trust framework for accurate intrusion detection, adaptive access control, and low latency threat response in today's cloud-based SaaS environments still exists.

III. Methodology

Fig. 1 proposed methodology presents a Zero Trust Security Framework for cloud-based SaaS applications using deep learning–based intrusion detection techniques for continuous verification and real-time threat detection. The CICIDS2017dataset is used to analyze both benign and malicious network traffic containing attacks. Data pre-processing involved merging datasets, removing irrelevant and non-numeric features, handling missing and infinite values, applying binary label encoding, and normalizing features using StandardAero. To address class imbalance, SMOTE is applied to the training dataset. Two deep learning models are developed: a DNN with Multi-Head Attention and an RNN-LSTM with self-attention for learning complex traffic patterns and sequential attack behavior. The models are evaluated using acc, prec, rec, F1score, AUC-ROC, Confusion Matrices, and ROC curves. Finally, the trained models are integrated into a Zero Trust Security Engine that continuously monitors network traffic and classifies each request as based on the “never trust, always verify” principle, thereby enhancing SaaS security through intelligent and adaptive threat detection.

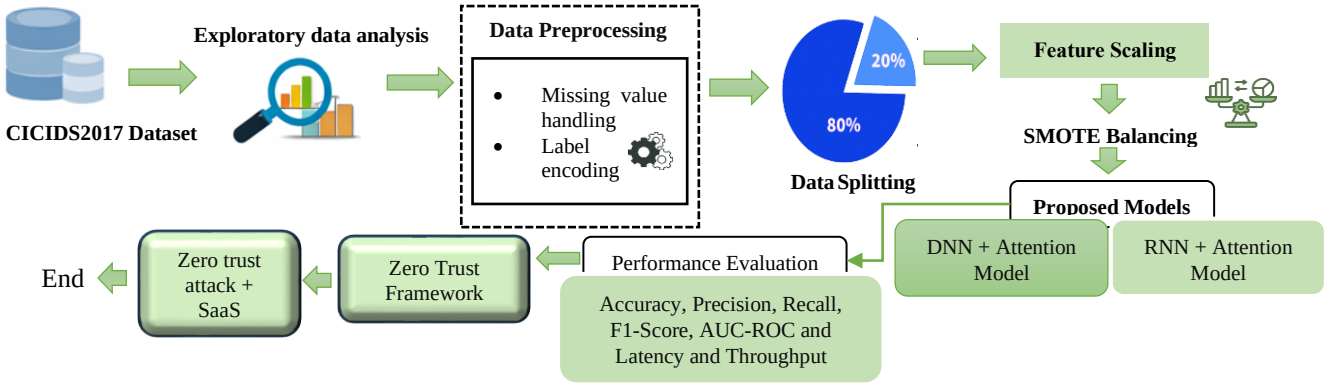

Fig. 1. Zero Trust Security Framework using Machine Learning

A. *Dataset Collection and Environment Setup*

The implementation began by installing the required Python libraries, including TensorFlow, Scikit-learn, Pandas, NumPy, Matplotlib, Seaborn, and Imbalanced-learn. The CICIDS2017 dataset is selected because it contains realistic benign and malicious network traffic representing modern cyberattacks such as DDoS, PortScan, Botnet, Web Attacks, Brute Force, and Infiltration. Eight CSV traffic files are loaded, including Friday-WorkingHours-Afternoon-DDos, PortScan, Monday-WorkingHours, Tuesday-WorkingHours, and Wednesday-WorkingHours. All files are merged into a single dataset and shuffled randomly. From the combined dataset, 10,000 samples are selected using random_state=42 to ensure reproducibility and computational efficiency.

B. *Data Preprocessing and Cleaning*

After loading the dataset, pre-processing operations are performed to improve Data Quality and model performance. The label column is automatically detected and binary encoding is applied where BENIGN = 0 and all attack categories are assigned 1. Non-numeric attributes and irrelevant columns are removed, while only numerical features are retained for analysis. Infinite values (+inf and -inf) and missing values (NaN) are are replaced using median imputation to maintain consistency. Zero-variance features with no useful information are removed to reduce dimensionality and computational overhead. Finally, the cleaned feature matrix and binary target labels are prepared for machine learning analysis.

C. *Exploratory Data Analysis (EDA)*

EDA is conducted to understand traffic behavior and feature relationships. These visualizations helped in understanding attack behavior patterns and feature dependencies within the dataset.

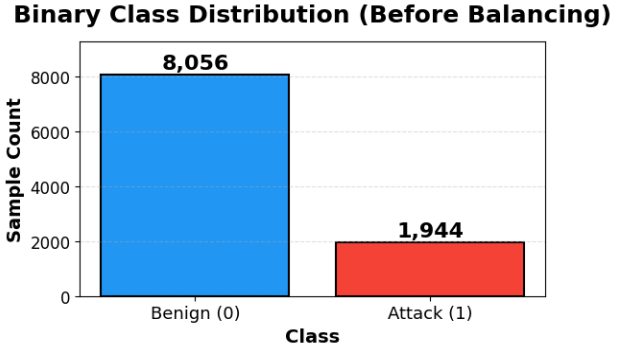

Fig. 2. Binary Class Distribution Before Data Balancing

Before applying balancing technique, the dataset binary class distribution is shown in Fig. 2. There is a high class imbalance in the data set, with 8,056 benign samples and 1,944 attack samples. This imbalance can favor the learning of majority class and thus can affect the intrusion detection performance. For this reason, balancing techniques like SMOTE are used to enhance the fairness of the model and the ability to detect attacks in the context of Zero Trust security.

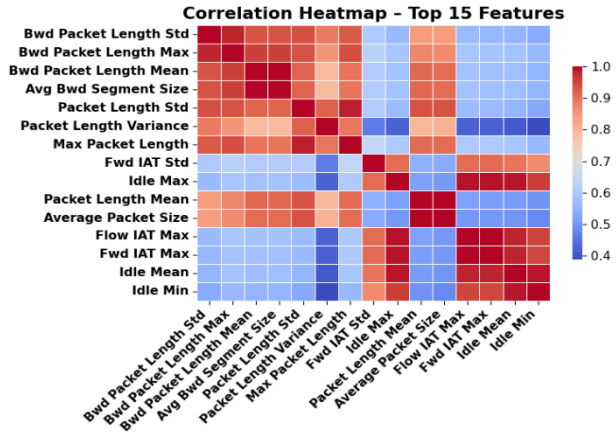

Fig. 3. Correlation Heatmap of Top 15 Selected Features

Fig. 3 presents the CorrelationHeatmap of the top 15 important features extracted from the intrusion detection dataset. The heatmap illustrates the relationships among packet length, flow IAT, and idle-time features using correlation coefficients. Strong positive correlations are represented by darker red shades, while weaker correlations are shown in blue shades. This analysis helps identify highly related features and supports effective FeatureSelection for improving the performance of the proposed Zero Trust security models.

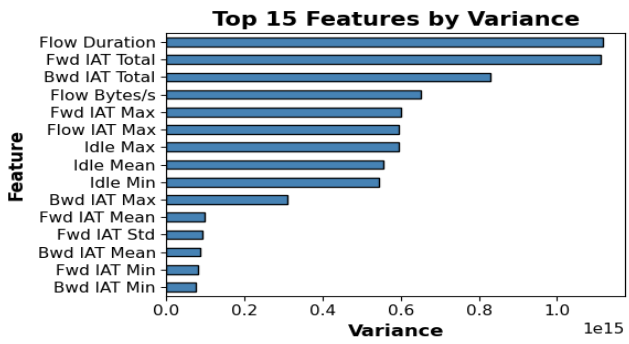

Fig. 4. Top 15 Features Ranked by Variance

Fig. 4 illustrates the top 15 most significant features selected based on variance analysis from the intrusion detection dataset. Features such as FlowDuration, Fwd IAT Total, and Bwd IAT Total exhibit the highest variance, indicating strong discriminatory capability for identifying malicious and benign traffic patterns. The suggested Zero Trust DL models benefit from this feature significance analysis, which aids in successful feature selection.

D. Data Splitting and Feature Scaling

The preprocessed dataset containing 10,000 network traffic samples with 68 numerical features is divided into training and testing sets using an 80:20 ratio with stratified sampling to preserve an original ClassDistribution. As a result, the training set consisted of **8,000 samples with 68 features** (8000, 68), while the testing set contained **2,000 samples with 68 features** (2000, 68). After splitting, feature normalization is performed using the **StandardScaler** technique to standardize all feature values around ZeroMean and UnitVariance. The StandardScaler transformation is mathematically represented as Equation (1):

$$z = \frac{x-\mu}{\sigma} \tag{1}$$

Where: x = OriginalFeatureValue, μ = meanof the FeatureValues, σ= StandardDeviation of the FeatureValues and z= standardized FeatureValues. This scaling procedure guarantees that each input feature has an equal impact on the training of the DL model.

E. Class Balancing using SMOTE

Since the CICIDS2017 dataset is highly imbalanced, the SMOTE is applied only to the Training Data. SMOTE generated synthetic attack samples for minority classes to create a balanced dataset and improve intrusion detection capability. The SMOTE synthetic sample generation formula is expressed as:

The SMOTE synthetic sample generation formula is expressed as Equation (2):

$$x_{new} = x_i + \lambda(x_{nn} - x_i) \tag{2}$$

Where: x_i= MinorityClass sample, x_{nn}= nearest neighbor of the minority sample, λ= RandomValue between 0 and 1 and x_{new} = newly generated synthetic sample. Before balancing, the training dataset contained 6,445 benign samples and 1,555 attack samples. After applying SMOTE, the minority attack class is oversampled to match the majority class distribution, resulting in 6,445 benign samples and 6,445 attack samples, shows in Fig. 5.

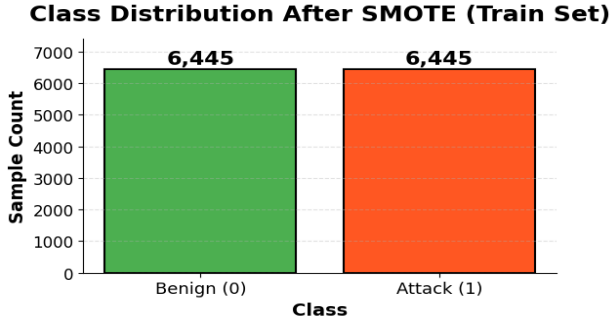

Fig. 5. Bar graph of after SMOTE

This process improved class balance, reduced model bias toward benign traffic, and enhanced the capability of the deep learning models to correctly identify malicious network activities.

F. DNN with Multi-Head Attention Model

The first proposed model is a DNN integrated with a Multi-Head Attention mechanism. DNNs are effective for intrusion detection because they can learn Complex Patterns from Network Traffic data. In the proposed framework, a DNN integrated with a Multi-Head Attention Mechanism is developed to improve contextual feature learning and attack detection performance. The architecture consisted of DenseLayers with **256, 128, and 64 neurons** using the **ReLU activation function** Equation (3)**:**

$$f(x) = \max(0, x) \tag{3}$$

Dropout layers with rates of **0.3** and **0.2** are used to reduce overfitting. A **Multi-HeadAttention** layer with **4 attention heads** and key_dim = 32 is applied to focus on important traffic features. The attention mechanism is defined as Equation (4):

$$\text{Attention}(Q, K, V) = \text{Softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{4}$$

where Qrepresents queries, Krepresents keys, Vrepresents values, and $d_k$is the key dimension. The model's capacity to detect hidden attack patterns and feature dependencies in NetworkTraffic is enhanced by this method. The final output layer used the Sigmoid activation function for binary classification of benign and malicious traffic Equation (5):

$$\sigma(x) = \frac{1}{1+e^{-x}} \tag{5}$$

The model is trained using Adam Optimizer with a Learning Rate of 0.001 and a binary cross-entropy loss function. Training is performed for 50 epochs with a BatchSize of 64, while Early Stopping and ReduceLROnPlateau callbacks are used to improve convergence and avoid overtraining.

G. RNN-LSTM with Self-Attention Model

The second proposed model utilized a RNN with LSTM and self-attention mechanisms to capture sequential attack behavior. In the proposed framework, an RNN integrated with LSTM and Self-Attention Mechanisms is developed to capture sequential attack behavior and long-term traffic dependencies. The architecture consisted of two LSTM layers with 128 and 64 units, respectively. The LSTM mechanism is represented as Equation (6):

$$h_t = f(Wx_t + Uh_{t-1} + b) \tag{6}$$

where x_t is the Current Input, h_{t-1} is the previous HiddenState, and $h_t$is the updated hidden state.

To enhance contextual learning, a Multi-Head Self-Attention layer with 4 attention heads and key_dim = 16 is applied to focus on important sequential traffic patterns and dependencies. GlobalAveragePooling1D is then used to reduce sequence dimensions before classification. Dense and dropout layers are added to improve generalization and reduce overfitting. The final Output Layer used the Sigmoid activation function for Binary Classification of benign and malicious traffic.

The model is trained using the Adam optimizer and the Binary Cross-Entropy loss function, defined as Equation (7):

$$L = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (7)$$

where y_i denotes the True Label and $\hat{y}_i$ denotes the forecasted probability. Training is performed using a Batch Size of 64 for 50 epochs. The input data is reshaped into three-dimensional tensors (samples, features, 1) to support sequential learning and temporal feature extraction.

H. Experimental Setup

The tests were carried out on a Lenovo Legion Pro Core i9-13900HX PC running Windows 10 with 32 GB of RAM and a processor speed of 3.90 GHz. It also made use of the NVIDIA GeForce RTX 4070 GPU to speed up processing. Python modules such as Pandas, Numpy, TensorFlow, and Keras were used.

I. Model Evaluation and Performance Analysis

Both deep learning models are evaluated using multiple classification and operational metrics including Accuracy, Precision, Recall, F1Score, AUC-ROC, Training Time, Prediction Time, Throughput, and Latency, discussed in Table I. Confusion matrices are generated to analyze true positives (TP), false positives (FP), false negatives (FN), and true negatives (TN). AUC-ROC evaluates the model's ability to distinguish between benign and malicious traffic across different threshold values. Higher AUC values indicate better classification performance.

TABLE I. PERFORMANCE EVALUATION MEASURES AND MATHEMATICAL FORMULAS

Measure	Definition	Formula
Accuracy	Measures the overall percentage of correctly classified samples.	Accuracy $= \frac{TP + TN}{TP + TN + FP + FN}$
Precision	Measures how many predicted attacks are actually attacks.	Precision $= \frac{TP}{TP + FP}$
Recall	Measures the ability to correctly detect malicious traffic.	Recall $= \frac{TP}{TP + FN}$
F1-Score	Harmonic mean of Precision and Recall.	$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$
Training Time/ Prediction Time	Training Time represents the total time required to train the model, while Prediction Time measures the time needed for intrusion prediction on test samples.	Throughput $= \frac{\text{Number of Samples}}{\text{Prediction Time}}$
Throughput	Number of samples processed per second.	Latency $= \frac{\text{Prediction Time}}{\text{Number of Samples}}$
Latency	Average prediction delay per sample.	Latency $= \frac{\text{Prediction Time}}{\text{Number of Samples}}$

IV. RESULTS AND DISCUSSION

The performance between the proposed DNN + Attention and RNN + Attention model for the Zero Trust security enforcement in SaaS environment is compared and presented in Table II. The DNN + Attention model showed the best performance in terms of real-time threat detection, with the highest accuracy (97.00%), F1-score (92.75%), and AUC-ROC (99.63%) while having the lowest latency and the fastest prediction time. The RNN + Attention model did well in terms of recall accuracy but it is computationally more complex due to its higher training time and latency. The DNN + Attention model is overall more efficient and effective at intelligent Zero Trust security monitoring and policy enforcement.

TABLE II. PERFORMANCE OF PROPOSED MODELS FOR ZERO TRUST SECURITY

Model Name	Accuracy	Precision	Recall	F1-Score	AUC-ROC	Training Time (s)	Prediction Time (s)	Throughput	Latency
DNN + Attention	0.9700	0.8747	0.9871	0.9275	0.9963	105.1774	0.8167	2449.0062	0.4083
RNN + Attention	0.8965	0.6602	0.9640	0.7837	0.9759	976.2583	4.1860	477.7847	2.0930

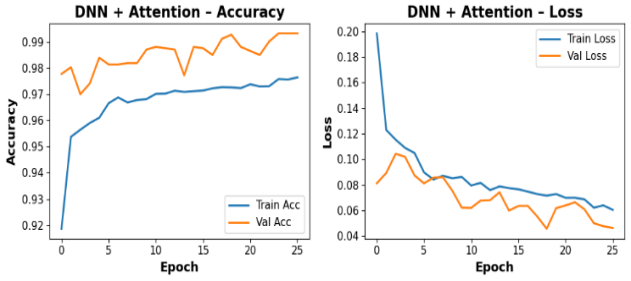

Fig. 6. Training and Validation Accuracy/Loss Curves of the DNN + Attention Model

Fig. 6 displays the training and validation performance, across several epochs, of the suggested DNN + Attention model. The accuracy graph reveals consistent learning progress over time, with high accuracy levels close to 98% both during training and validation, suggesting successful learning and good generalization. At the same time, the loss graph shows a steady decrease in Training Loss and Validation Loss, indicating a stable convergence with a decrease in prediction error throughout the training process.

Fig. 7 displays the training and validation performance, as a function of epoch count, of the suggested RNN + Attention model. The accuracy curves indicate that the models gradually learn and stabilize around 95% accuracy, demonstrating their ability to learn sequentially. The loss curves show a general decrease in training and testing loss, with some minor variations in the losses over time, as expected with an RNN model.

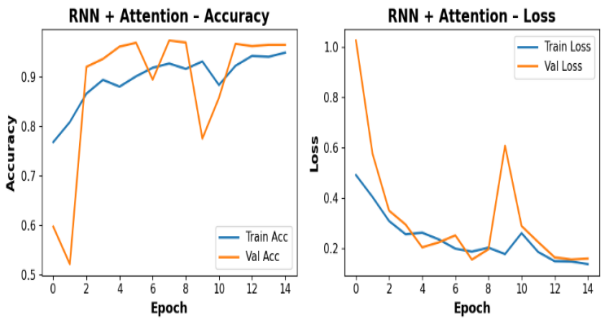

Fig. 7. Training and Validation Accuracy/Loss Curves of the RNN + Attention Model

The confusion matrices for Zero Trust intrusion detection problem model DNN + Attention and model RNN + Attention are presented in Fig. 8. The DNN + Attention model outperformed the RNN + Attention model in terms of the number of correct predictions of benign events (1556) and correctly detected attacks (384), and had fewer FP and FN predictions. The RNN+Attention model also exhibited an excellent attack detection ability, but produced more misclassifications. In summary, DNN+Attention demonstrated improved classification accuracy and consistent security decision-making in the protection of SaaS applications.

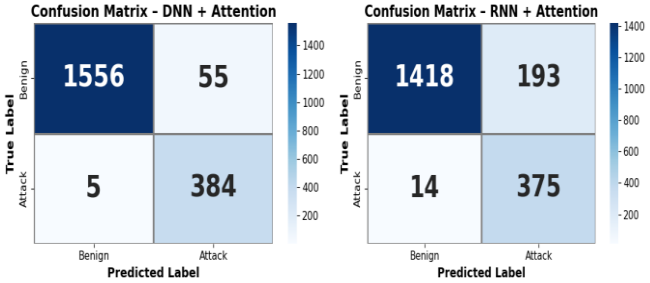

Fig. 8. Confusion Matrix of DNN + Attention and RNN + Attention Models

Fig. 9 illustrates the ROC curve comparison between the DNN + Attention and RNN + Attention models for Zero Trust intrusion detection. The DNN + Attention model obtained the highest AUC-ROC score of 0.9963, outperforming the RNN + Attention model with an AUC of 0.9759. The high TPR and low FPR shown by the curves that stay near to the top-left corner prove that the suggested models are effective for monitoring secure SaaS applications.

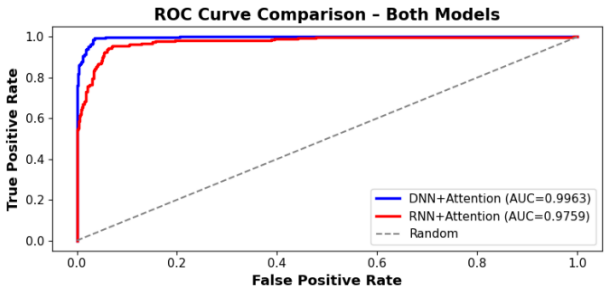

Fig. 9. ROC Curve of DNN + Attention and RNN + Attention Models

Finally, the performance comparison of the DNN + Attention and RNN + Attention models in the proposed Zero Trust Security Framework is presented in Table III. The DNN + Attention model showed the highest accuracy (97.00%), F1-score (92.75%) and AUC-ROC (99.63%) values, and it also had the lowest latency and fastest prediction time. The Zero Trust framework is not siloed, and the models deployed are policy engines that would continuously review network flows, and make ALLOW/ DENY/QUARANTINE decisions dynamically based on threat level.

TABLE III. FINAL PERFORMANCE COMPARISON OF DEEP LEARNING MODELS IN THE ZERO TRUST SECURITY FRAMEWORK

Model Name	Accuracy	Precision	Recall	F1-Score	AUC-ROC	Training Time (s)	Prediction Time (s)	Throughput	Latency
DNN + Attention	0.9700	0.8747	0.9871	0.9275	0.9963	105.1774	0.8167	2449.0062	0.4083
RNN + Attention	0.8965	0.6602	0.9640	0.7837	0.9759	976.2583	4.1860	477.7847	2.0930

The proposed Zero Trust Engine is evaluated for the purpose of SaaS application security in Table IV, based on the DNN + Attention and RNN + Attention models. Both models handled 2000 API requests, and dynamically applied ALLOW/DENY/QUARANTINE security decisions. The RNN + Attention model had slightly better rate of threat detection (30.85%) and overall security score (52.14%), while the DNN + Attention model had a higher legitimate pass rate (79.21%) but produced fewer false alarms. The results illustrate the effectiveness of leveraging deep learning models as intelligent policy enforcement engines in Zero Trust SaaS security architectures.

TABLE IV. SAAS APPLICATION SECURITY METRICS EVALUATION UNDER ZERO TRUST ENGINE

Security Metrics	DNN + Attention	RNN + Attention
Total API Requests	2000.00	2000.00
Threats Detected (TP)	89.00	120.00
Legitimate Passed (TN)	1276.00	1183.00
False Alerts (FP)	335.00	428.00
Missed Attacks (FN)	300.00	269.00
Threat Detection Rate (%)	22.88	30.85
False Alert Rate (%)	20.79	26.57
Session Block Rate (%)	21.20	27.40
Legitimate Pass Rate (%)	79.21	73.43
Attack Containment (%)	22.88	30.85
Zero-Day Escape Rate (%)	77.12	69.15
Overall Security Score (%)	51.04	52.14

The proposed DNN + Attention and RNN + Attention models are compared with the previous intrusion detection approaches in Table V. The DNN + Attention model performed best overall with 97.00% accuracy and 92.75% F1-score, whereas BiGAN, NB, OCSVM and DeepGFL models are not able to achieve such results. The RNN + Attention model is also able to achieve high accuracy and recall scores at 89.65% and 96.40% respectively. The results have validated the ability of the proposed deep learning models with attention mechanism for Zero Trust SaaS security and intelligent intrusion detection.

TABLE V. COMPARATIVE PERFORMANCE ANALYSIS WITH EXISTING INTRUSION DETECTION MODELS

Model Name	Accuracy	Precision	Recall	F1-Score
DNN + Attention	0.9700	0.8747	0.9871	0.9275
RNN + Attention	0.8965	0.6602	0.9640	0.7837
BiGAN [23]	0.823		0.763	
NB[24]	0.8083	0.8556	0.8083	0.7948
OCSVM[25]	0.8356	0.6525	0.4784	0.5520
DeepGFL[26]	0.531		0.448	0.531

The proposed Zero Trust Security Framework a combination of DNN + Attention and RNN + Attention models is proposed for intelligent intrusion detection in SaaS environments. The framework continually scans the network traffic and dynamically enforces security decisions, like ALLOW or DENY/QUARANTINE, depending on the level of threat detected. The attention mechanisms enable the models to capture the relevant traffic patterns, thereby boosting their accuracy of detection, minimizing false positives, and aiding in the effective monitoring of traffic in real time for security purposes. DNN + Attention demonstrated the best accuracy, lowest latency, and prediction

speed, outperforming the other models proposed, which is very desirable for modern Zero Trust cloud security applications.

A. Justification and Novelty of this Study

The proposed work is justified because the need for intelligent and adaptive security mechanism in the cloud-based SaaS environment, which is being unable to secure using the traditional security models, is ever increasing due to cyber threats. The novelty of this framework lies in the implementation of attention-based DNN and RNN models in a single framework of Zero Trust to detect intrusions and enforce policies at runtime through ALLOW and DENY/QUARANTINE decisions. Also, the framework integrates feature optimization, adaptive traffic analysis and intelligent threat monitoring to increase detection accuracy, lower false alarms, and provide enhanced SaaS security management in real-time.

B. Limitations of this Study

The suggested Zero Trust Security Framework had good intrusion detection capabilities, but there are still some drawbacks. The framework is tested largely using benchmark datasets that may not capture all the dynamic SaaS traffic conditions. In addition, the RNN+Attention model also had higher computational complexity and a longer training time, potentially impacting the efficiency of large-scale deployment. Furthermore, the framework is currently designed for supervised learning for threat detection and may need to be further improved to deal with real-time cloud environments and adaptive adversarial threats and highly evolving zero-day attacks.

V. Conclusion

In today's fast-changing cybersecurity landscape, cloud computing and SaaS applications are a large part of the challenge regarding access control and real-time threat detection. Traditional security approaches are often unable to effectively handle dynamic and sophisticated cyberattacks, thereby increasing the need for intelligent ZeroTrust architectures. The present paper proposed an intelligent Zero Trust Security Framework that combined with DNN + Attention and RNN + Attention models to detect intrusion and adaptively modify the security policies. The proposed framework is designed to monitor network traffic continuously and to dynamically determine whether the requests are legitimate or malicious, based on ALLOW or DENY/QUARANTINE decisions. Experimental results are shown to achieve the best performance with DNN+Attention with the accuracy of 97.00%, the F1-score of 92.75%, the AUC-ROC of 99.63% and the lower latency, faster prediction time compared to the other models. The proposed framework for intelligent SaaS security monitoring is also proven effective through comparative analysis with the existing approaches. For future research, transformer-based architectures, federated learning, explainable AI, and adaptive policy optimization may be tested for greater scalability, preservation of privacy, and detection of zero-day attacks in large systems within the cloud.

References

[1] O. S. Adanigbo, D. Kisina, O. E. Akpe, S. Owoade, B. C. Ubamadu, and T. P. Gbenle, "A conceptual framework for implementing zero trust principles in cloud and hybrid IT environments," *IRE Journals (Iconic Res. Eng. Journals)*, vol. 5, no. 8, pp. 412–421, 2022.

[2] D. Jain and S. Jain, "Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395685.

[3] V. K. Bollu, "Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and Security Implications," *World J. Adv. Res. Rev.*, vol. 29, no. 1, pp. 285–294, 2026, doi: 10.30574/wjarr.2026.29.1.0007.

[4] B. P. Singh, "Convergence of AI and Zero Trust: Enabling Continuous Verification Across Hybrid Cloud Environments," *Int. J. Intell. Syst. Appl. Eng.*, vol. 14, no. 1s, pp. 339–348, Apr. 2026, doi: 10.17762/ijisae.v14i1s.8181.

[5] S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in *2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

[6] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," *Sustainability*, vol. 14, p. 11213, 2022, doi: 10.3390/su141811213.

[7] H. P. Cyril and S. Kumara, "Identification of Anomalies via Deep Learning-Based Models for High-Dimensional Telecom Traffic Data," *J. Adv. Artif. Intell.*, vol. 4, no. 1, pp. 24–37, February, 2026, doi: 10.18178/JAAI.2026.4.1.24-37.

[8] P. Naayini and S. Kamatala, "Automating Infrastructure Platforms with Cloud , Kubernetes , and Site Reliability Engineering," *Int. J. Comput. Tech.*, vol. 8, no. 6, pp. 1–9, 2021, doi: 10.5281/zenodo.15634257.

[9] K. Jangiti, "Design and Validation of a Machine Identity Governance Framework for AI Agents in Multi-Cloud Environments," in *SoutheastCon 2026*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/SoutheastCon63549.2026.11476363.

[10] V. Sanikal, "AI-Enhanced Network Security Framework for Cloud-Edge Integrated Environments," in *2026 Innovations in Machine, Engineering, and Digital Conference (IMED)*, 2026, pp. 1–6. doi: 10.1109/IMED68921.2026.11484417.

[11] J. B. Mehta, "Autonomous Patch Validation For Zero-Day Exploits In Enterprise Clouds," *Int. J. Appl. Math.*, vol. 38, no. 4s, pp. 1270–1285, August, 2025, doi: 10.12732/ijam.v38i4s.685.

[12] S. Tiwari, W. Sarma, and A. Srivastava, "Integrating Artificial Intelligence with Zero Trust Architecture: Enhancing Adaptive Security in Modern Cyber Threat Landscape," *Int. J. Res. Anal. Rev.*, vol. 9, no. 2, p. 712, 2022.

[13] R. Lingam, S. Nagi, M. Chigurupati, and B. T. Myneni, "Resilient DevSecOps: Self-Healing Cloud-Native Systems via SRE-Driven AI Threat Detection and Response," in *2026 International Conference on Smart Futuristic Technology*, IEEE, Jan. 2026, pp. 1–6. doi: 10.1109/ICSFT66733.2026.11508049.

[14] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.

[15] S. Mishra, T. S. M. Aldafas, and N. S. Alshammari, "A zero-trust digital twin framework for privacy-preserving multi-dataset intrusion detection in industrial IoT with lightweight blockchain auditing," *Sci. Rep.*, vol. 16, no. 1, p. 15236, Mar. 2026, doi: 10.1038/s41598-026-42041-w.

[16] V. B Maniyat and A. Kumar B R, "Adaptive Threat Modeling with MITRE ATT&CK: A Machine Learning Framework for Real-Time Adversarial Detection," in *2025 9th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSITSS67709.2025.11295603.

[17] M. Al-Zewairi, S. Almajali, M. Ayyash, M. Rahouti, F. Martinez, and N. Quadar, "Multi-Stage Enhanced Zero Trust Intrusion Detection System for Unknown Attack Detection in Internet of Things and Traditional Networks," *ACM Trans. Priv. Secur.*, vol. 28, no. 3, pp. 1–28, Aug. 2025, doi: 10.1145/3725216.

[18] A. Jain, A. A. Alya, E. J. Parkash, P. Kaur, A. Singh, and Kamal, "Zero Trust Edge: An Explainable AI-Driven Energy- Aware IIoT Framework with Zero Trust Security for Sustainable Smart Grid,"

in *2025 IEEE 2nd International Conference on Green Industrial Electronics and Sustainable Technologies (GIEST)*, IEEE, Oct. 2025, pp. 1–6. doi: 10.1109/GIEST66547.2025.11387523.

[19] F. Guo, H. Jiao, X. Zhang, Y. Zhou, and H. Feng, "Information Security Network Intrusion Detection System Based on Machine Learning," in *2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024*, 2024. doi: 10.1109/ICDSNS62112.2024.10691041.

[20] M. Dhinakaran, M. Sundhari, S. Ambika, V. Balaji, and R. T. Rajasekaran, "Advanced Machine Learning Techniques for Enhancing Data Security in Cloud Computing Systems," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, 2024, pp. 1598–1602. doi: 10.1109/IC2PCT60090.2024.10486559.

[21] H. Teymourlouei, "A Machine Learning Approach to the Evaluation of Zero Trust Compliance in Network Infrastructure," in *International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2023*, 2023. doi: 10.1109/ICECCME57830.2023.10253205.

[22] J. B. Mehta, "Securing Test Automation in Zero Trust Architectures: A Framework for Continuous Verification," in *2025 International Conference on Computer and Applications (ICCA)*, IEEE, Dec. 2025, pp. 1–5. doi: 10.1109/ICCA66035.2025.11430950.

[23] M. Deng, C. Sun, Y. Kan, H. Xu, X. Zhou, and S. Fan, "Network Intrusion Detection Based on Deep Belief Network Broad Equalization Learning System," *Electronics*, vol. 13, no. 15, p. 3014, Jul. 2024, doi: 10.3390/electronics13153014.

[24] D. Haider, S. Mushtaq, H. Ali, and M. Mohd Su'ud, "Enhancing Zero Trust Cybersecurity using Machine Learning and Deep Learning Approaches," *J. Informatics Web Eng.*, vol. 4, no. 3, pp. 24–34, Oct. 2025, doi: 10.33093/jiwe.2025.4.3.2.

[25] Z. Xu and Y. Liu, "Robust Anomaly Detection in Network Traffic: Evaluating Machine Learning Models on CICIDS2017," 2025.

[26] M. Sahu, "Data Analytics Approaches for Effective Threat Identification in Cloud Databases," *Int. J. Emerg. Res. Eng. Technol.*, vol. 7, no. 2, pp. 1–9, 2026, doi: 10.63282/3050-922X.IJERET-V7I2P101.

