ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 4 Issue 3 September 2024 / Page No: 209-218
Paper Id: JETA-V4I3P122 / Doi: 10.56472/25832646/JETA-V4I3P122

Original Article

Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks

Gaurav Sarraf[1], Vibhor Pal[2]
[1,2] *Independent Researcher*

Received Date: 31 July 2024 Revised Date: 07 September 2024 Accepted Date: 29 September 2024

Abstract: *The zero-trust cloud networks decentralized and dynamic nature turns them into easy targets of advanced cyberattacks, and the traditional security controls are not sufficient anymore. This article introduces a self-sovereign cloud security model utilizing Convolutional Neural Network (CNN) to detect anomalies. Selected methodology utilizes CSE-CIC-IDS2018 dataset, and includes extensive preprocessing in terms of outlier elimination by Local Outlier Factor (LOF), Z-score outliers, and dimensionality reduction by Principal Component Analysis (PCA). The dataset is split into testing of 10% and 90% training data and CNN model is used to extract spatio-temporal patterns of network traffic to classify normal and malicious streams with high accuracy. It is shown through experimental findings which proposed model has a higher performance of 99.87 accuracy, 99.86% recall and precision, and a F1-score of 99.87, being better than benchmark models like the MLP-PSO, LSTM, and SVM. The findings demonstrate the strength, scalability, and usefulness of the model in offering real-time Anomaly Detection (AD) in zero-trust cloud networks.*

Keywords: *Zero-Trust Cloud Networks, Anomaly Detection, Local Outlier Factor (LOF), Patio-Temporal Patterns, Intrusion Detection, Cybersecurity, Machine Learning (ML), Deep Learning (DL).*

I. INTRODUCTION

The world is experiencing an upward trend in cybersecurity costs and cybercrimes. Hackers can exploit some loopholes in digital technologies; hence, companies should make sure that technological tools are not susceptible to computer attacks [1]. To ensure cybersecurity, networks and data are secured against malicious intent or unauthorized access through the use of authentication, encryption, and access control. Cybersecurity is the methods to guard against the unauthorized access and malicious activities of computers and networks like stealing and destroying data [2]. AD is a significant issue which is centuries-old. Several different techniques have been established and applied to identify abnormalities to various applications. AD is defined as issue of identifying the patterns in the data which are not expected to occur. Anomaly detection is a concept that has a very expansive range of applications. The relevance of abnormalities detection in the different areas of application regards the fact that unprotected data could possess an appropriate amount, vital, and an actionable information. An example of this is when an unusual traffic pattern of a computer network is detected, the attack of a compromised computer can be revealed [3][4]. The modern world of cybersecurity nowadays is constantly being assaulted by an ever-present onslaught of advanced cyber threats. The spread of IoT devices and subsequent growth of network security professionals poses additional difficulties as the scope of attacks expands and new issues come into scope. Such paradigm shift requires basic transformation in the way the organizations treat network security [5]. ZTNA has become a promising security model that removes shortcomings of traditional models. ZTNA works on premise of never trust, always verify, which in effect brings about down the road of an untested internal network based on implicit trust.

Digital infrastructure is currently supported by cloud networking, transforming the system of data storage, processing and accessibility to organizations [6][7]. The integration of cloud technologies dramatically affects the traditional architecture of security, requiring sophisticated measures in the direction of the protection of confidential data and integrity of digital systems. A major challenge in cloud networking system is the reduction of data storage and processing defects [8]. The zero trust cybersecurity strategy goes beyond a location-based approach and focusses on data in order to enhance security measures for users, data, systems, and assets that can evolve over time [9] [10]. There are threats both within and outside of a network, and zero trust security acknowledges this, says the National Institute of Standards and Technology. System management and cybersecurity are part of a unified plan.

Researchers, practitioners, and legislators have all taken an interest in the potential synergies between ZT technology and artificial intelligence (AI) in recent years. The synergy between AI and ZTA has produced remarkable improvements in real-time security operations [11]. One popular method for spotting outliers is machine learning (ML). This method of identifying outliers is the most common and traditional one. ML has achieved some success [12]. Among these methods, you may find supervised models that rely on labelled data, unsupervised models that rely on unlabelled data, and semi-supervised learning techniques that combine a large number of unlabelled with a small number of labelled datasets ones to identify

outliers [13]. There was extensive usage of ML and DL procedures for a variety of jobs [14], including classification, regression, and IoT applications like image analysis, intrusion detection, and recommendation systems.

A. Motivation and Contributions of the Study

The increasing prevalence of cybercrimes and the rapid expansion of digital infrastructures, particularly cloud and IoT environments, have significantly intensified the challenge of securing networks and data. Traditional cybersecurity models, which often rely on implicitly trusted internal networks, are insufficient to address sophisticated and evolving attack vectors. ZTNA has emerged as a robust paradigm, emphasizing "never trust, always verify," yet detecting anomalies in such dynamic environments remains a critical challenge due to high data volume, class imbalance, and complex attack patterns. This study is inspired by need to develop intelligent, scalable, and adaptive anomaly detection systems which leverage ML and DL procedures to enhance real-time threat detection, minimize false positives, and improve the overall resilience of cloud-based and IoT networks against cyberattacks. The key contributions offered by the study are discussed below:

- Making use of the robust and well-known CSE-CIC-IDS2018 dataset, which is used for research purposes with regard to the study of intrusion detection in networks.
- Implementation of a robust pre-processing pipeline along with outlier removal with LOF, data cleaning, and Z-score normalization to improve data quality and consistency.
- Application of PCA for feature selection to reduce dimensionality and enhance computational efficiency without compromising detection accuracy.
- Development of a CNN-based intrusion detection model capable of classifying normal and high accuracy of malicious traffic.
- Detailed performance analysis by recall, precision, accuracy, and F1-score loss that will provide a trusted rating of the model performance.

B. Significance of the Study

This study is important because it focuses on the increasing concern of cybersecurity threats in the contemporary networks where the complexity and volume of attacks are growing in complexity thus requiring more effective detection methods. Using CSE-CIC-IDS2018 dataset, that serves as a benchmark dataset in intrusion detection, and utilizing deep learning through CNN, the study helps create an automated, scalable and accurate intrusion detection system. The combination of outlier elimination, normalization and feature selection with PCA advance quality of data and lower calculation cost which allows faster and more accurate detection. The outcomes of this study can support organizations in strengthening network security, minimizing false alarms, and improving real-time threat response, thereby contributing to safer digital infrastructures.

C. Organization of the Study

Here is how paper is planned: A full survey of relevant literature on anomaly detection in Zero-Trust cloud networks is provided in Section II. Section III describes the research methodology, including the dataset, pre-processing procedures, and the implementation of the CNN model. Part IV details the outcomes of the experiments and offers a thorough evaluation of the data. In Section V, review study's findings and discuss potential avenues for further investigation.

II. LITERATURE REVIEW

This article builds upon a critical evaluation and inclusive review of existing research on AD in Zero-Trust cloud networks, which served to refine its focus and shape the overall direction of the work.

Sharma, Chan and Leckie (2023) they compared its performance to that of a conventional Distributed CIDS and an earlier suggested Hybrid CIDS, basing their evaluation on network overhead and detection accuracy. Analysing real-world application cluster's telemetry data, their ground-breaking CIDS increased detection 99.4% accuracy and decreased 51.8% network overhead when testing for anomalies in service endpoint interactions, service path interactions, HTTP methods, and numerical value's unusual variance containing traffic processing duration, response size, request size [15].

Hassan et al. (2023) The InSDN dataset is utilized to evaluate proposed framework with several learning models, including RF, AB, KNN, NB, DT, and LR classifiers for LR, RF, and NB. In comparison to AB, RF, NB, KNN, LR, DT, and LSTM classifiers—which achieved 95%, 88%, 97%, 93%, 90%, 98%, and 88.31% accuracy levels, respectively— In terms of data classification of multi-class attack, the outcomes demonstrate that proposed Deep CNN model achieves a maximum 99.85% accuracy [16].

Khan and Mailewa (2023) assessed in depth the 4 types of attacks found in the NSL-KDD dataset: R2L, U2R, DoS, and Probe. They showed that DAE-SVM was much better at classifying than PCA-SVM; their model detected low-frequency attacks better than the baseline models (micro-average score 0.72 vs. 0.63 for PCA-SVM). For binary classes, the optimal model was

DAE-SVM with L1 penalty (145 seconds for training and testing), but in the multi-class situation, DAE-SVM without penalty term was superior (PCA-SVM takes 300 seconds whereas 142.62 seconds) [17].

Vinolia, Kanya and Rajavarman (2023) goal of this study is to examine ways in which DL and ML networks are utilised by a variety of approaches at different phases of the intrusion detection process so that can improve our outcomes. According to results of experiments, strategies which are based on deep learning and do not require supervision obtain an accuracy rate of 99.95% [18].

Yunanto and Pao (2022) enables an enhanced access control system to assess the potential dangers posed by each and every user's actions throughout day-to-day operations. Our study focusses on user behaviour risk evaluation by making use of log entries that are recorded by Apache Web Server. This is done in order to describe how users interact with the server of the organisation. Although this method has proven effective in other contexts, it has never been planned to handle Apache Access log data. We suggest a different approach to conducting and evaluating experiments for User abnormal behaviour identification as our log analysis dataset differs from others in that it does not contain labels defined by domain experts [19].

Srinivasan et al. (2021) proposes developing an Anomaly detection system to keep an eye out for any unusual or questionable behaviour on the network, as well as a system to categorise connected devices as either IoT or non-IoT using ML. To ensure the ML model is efficient, it will be put to use on a test bed including both IoT and non-IoT devices, as well as a connector and hub. A dataset was used to train the model. In order to evaluate how well various ML techniques work, we shall compute the F-measure [20].

Satam, Satam and Hariri (2020) assessed the efficacy of various ML algorithms in distinguishing between typical and non-standard Bluetooth protocol flows; Bagging, Ad boost, C4.5, SVM, Naive Bayes, and Jrip were among these algorithms. As much as 99.6 percent recall and precision can be achieved by the ABIDS in detecting attacks on Bluetooth protocols. Device whitelisting is another feature of the ML-BIDS architecture that helps prevent unauthorised devices from joining to the Bluetooth network [21].

Table 1 delivers a comprehensive summary of recent studies on AD in Zero-Trust cloud networks, outlining their applications, methodologies, datasets, performance metrics, and limitations.

Table 1 : Recent Studies on AD in Zero-Trust Cloud Networks

Author (Year)	Application	Technique / Dataset	Performance	Limitations / Future Work
Sharma, Chan & Leckie (2023)	Distributed CIDS in real-world application clusters	Novel CIDS using telemetry data	99.4% detection accuracy, 51.81% lower network overhead	Limited to service path/endpoint anomalies; requires validation on broader datasets
Hassan et al. (2023)	Intrusion detection in SDN	Deep CNN vs. RF, AB, KNN, NB, DT, LR, LSTM on InSDN dataset	CNN achieved 99.85% accuracy; others between 88–98%	Needs testing on larger real-world SDN datasets; model complexity may impact scalability
Khan & Mailewa (2023)	NSL-KDD attack detection (U2R, DoS, R2L, Probe)	DAE-SVM vs. PCA-SVM	DAE-SVM micro-average 0.72 vs. 0.63; faster training (142.62s vs. 300s)	Limited to NSL-KDD dataset; future work on real-time attack detection
Vinolia, Kanya & Rajavarman (2023)	Intrusion detection using DL & ML	Unsupervised DL-based techniques	Achieved accuracy of 99.95%	Lacks dataset diversity; future work to validate on heterogeneous networks
Yunanto and Pao, (2022)	User behavior risk evaluation from Apache logs	Log analysis (Apache Access Log)	Alternative method proposed for unlabeled data	Dataset lacks expert labeling; future extension needed for ground-truth validation
Srinivasan et al., (2021)	Device classification & anomaly detection	ML models on IoT & Non-IoT testbed	Performance evaluated via F-measure	Needs deployment in real-world large-scale IoT environments
Satam, Satam & Hariri (2020)	Bluetooth protocol attack detection	ML-BIDS framework with C4.5, SVM, AB, Jrip, NB, Bagging	ABIDS achieved precision & recall of 99.6%	Limited to Bluetooth networks; extendable to broader IoT wireless protocols

III. RESEARCH METHODOLOGY

The proposed methodology involves the use of CSE-CIC-IDS2018 dataset on Kaggle as a starting point of proposed methodology in terms of anomaly detection. Data cleaning, outlie ring with LOF, and Z-score normalization are utilized to pre-process data, and PCA is used to select features, reducing dimensionality. Training data will make up 90% of the total, while testing data will account for 10% and the classification of benign and malevolent traffic will be accomplished using a CNN model. Lastly, precision, F1-score, recall, accuracy, and loss are utlized to evaluate model and give a picture of the model effectiveness. The flow of methodology is shown in Figure 1.

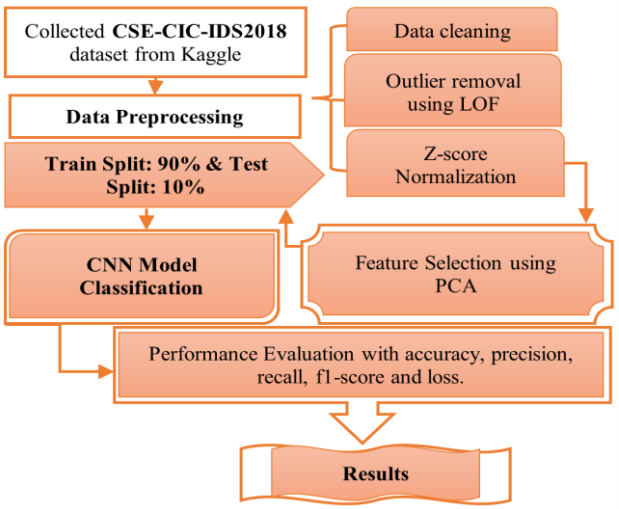

Figure 1 : Proposed flowchart for Anomaly Detection in Zero-Trust Cloud Networks

Next section describes the process represented in the proposed flowchart of the AD in Zero-Trust Cloud Networks.

A. Data Collection and Visualization

Collaborated on by the Communications Security Establishment (CSE), the Canadian Institute for Cyberspace (CIC), the CSE-CIC-IDS2018 dataset serves as a thorough and current standard for cyber intrusion detection. It encompasses 14 different attack traffic and benign traffic, intending on 7 different classes, namely Heartbleed, Force, Brute DDoS, Botnet, DoS, Web attacks and Infiltration, along with 80 features. Table 2: Statistical Information of the CSE-CIC IDS 2018 Dataset

A statistical summary of the CSE-CIC-IDS2018 data is presented in Table II, which shows the balance between the benign and malicious network traffic.

Table 2 : Statistical Information of the CSE-CIC IDS 2018 Dataset

Flow Type	No. instances	Ratio
Benign	14,097,779	83.6861%
SSH-brute force	187,589	1.1136%
All attacks	2,748,235	16.3139%
Infiltration	161,934	0.9613%
SQL injection	87	0.0005%
Dos attack-slowloris	10.990	0.0652%
FTP-brute force	193,360	1.1478%
Dos attack-Hulk	461,912	2.7420%
Dos attacks-SlowHTTPTest	139,890	0.8304%
DDoS attack-LOIC-UDP	1.730	0.0103%
DoS attack-GoldenEye	41,508	0.2464%
DDoS attack-HOIC	686,012	4.0723%
DDoS attack-LOIC-HTTP	576,191	3.4203%
Brute Force-Web	611	0.0036%
Brute Force-XSS	230	0.0014%
Bot	286.191	1.6989%
Total	16,846,014	100%

The dataset contains over 16 million instances, with benign traffic comprising the majority at approximately 84%, while malicious traffic accounts for around 16%. Among the attack types, DDoS variants such as HOIC and Hulk are the most prevalent, whereas attacks like SQL injection, DDoS-LOIC-UDP, and Brute Force-XSS are relatively rare. This distribution underscores the significant class imbalance inherent in the dataset, reflecting the challenges of detecting low-frequency attacks in real-world network environments. Some EDA of the dataset are shown below:

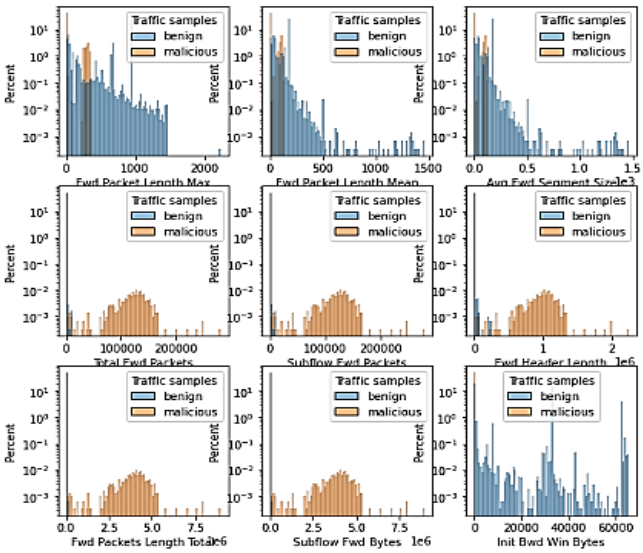

Figure 2 : Traffic Samples

Figure 2 shows nine histograms comparing benign (blue/gray) and malicious (orange) traffic distributions on a logarithmic scale. While features in the top row (e.g., 'Fwd Packet Length Mean', 'Fwd Packet Length Max') show significant overlap, the middle and bottom rows (e.g., 'Subflow Fwd Packets', 'Total Fwd Packets') display distinct malicious clusters. Notably, packet count-related metrics exhibit pronounced peaks for malicious traffic, making them effective for distinguishing between benign and malicious samples.

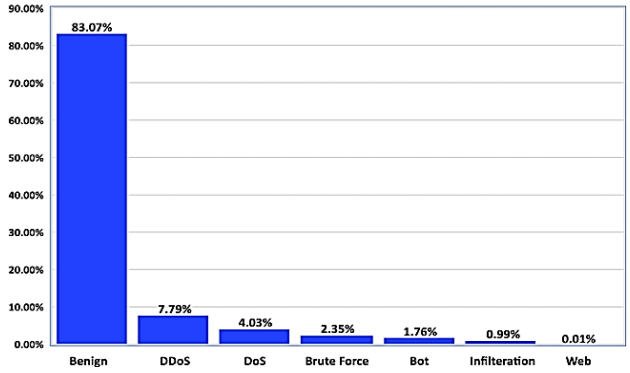

Figure 3 : Distribution of Attack Classes in CSE-CIC-IDS2018

Figure 3 presents a bar chart of dataset class distribution, showing a pronounced imbalance. The 'Benign' class dominates at 83.07%, while malicious traffic collectively accounts for less than 17%. Among attacks, DDoS is most frequent (7.79%), followed by Brute Force (2.35%), DoS (4.03%), Infiltration (0.99%), Bot (1.76%), and Web (0.01%). The chart highlights the dataset's heavy skew toward benign traffic, typical of real-world network environments.

B. Data Pre-Processing

Features like timestamps and IP addresses, which were present in the initial dataset, do not significantly affect the likelihood that the traffic is aberrant. The preprocessing steps are explained below:

a) Data Cleaning

Eliminating first four features "Src IP", —"Flow ID", "Src Port," and "Dst IP"—reduced the list to 80. The significance of these datasets dictated their selection, despite the fact that they have different feature counts. The dataset underwent homogenizing so as to have 80 features and eliminating the mentioned initial properties.

b) Outlier Removal using LOF

This study uses LOF, which is a density-based algorithm, in order to identify outliers in an efficient way, through studying the local density variations among data points. LOF score of a given point A is calculated as follows using the Equation (1):

$$LOF_k(A) = \frac{\sum B \in N_k(A) \frac{LRD(B)}{LRD(A)}}{|N_k(A)|} = \frac{\frac{\sum B \in N_k(A)}{|N_k(A)|}}{LRD(A)} \quad (1)$$

The LOF score is used to quantify the difference in density of a point and their neighbours.

c) Z-Score Normalization

This algorithm normalizes feature's values so that standard and mean deviation are 0 and 1 correspondingly. It is reached by taking mean of the feature out of each of the values and standard deviation's dividing result. This mathematical expression of this strategy is as follows Equation (2):

$$X' = \frac{(X - mean)}{std} \quad (2)$$

and where X is an original value and X^' is the normalized value.

C. Feature Selection using PCA

Data scientists and machine learning experts employ principal component analysis, a difficult statistical method, to simplify datasets. Its primary objective is to reduce the amount of attributes or dimensions in a dataset while keeping essential data [22]. One way principal component analysis does this is by creating a new collection of variables called principle components from the original set of variables. These components are intentionally designed uncorrelated so that we can capture maximum variability in data. They are just the initial characteristics combined in a linear fashion. By reducing the data to a more digestible and informative shape, principal component analysis (PCA) essentially streamlines data processing and interpretation.

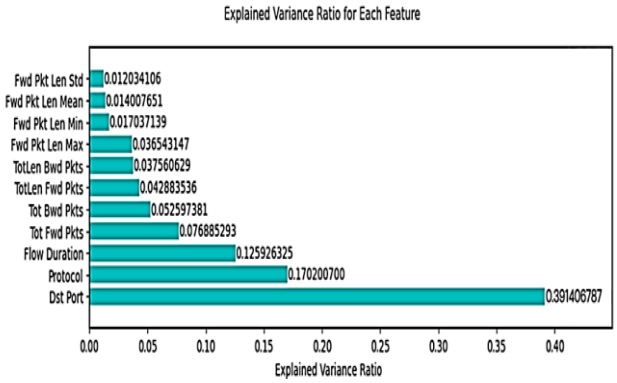

Figure 4 : Feature Selection by using PCA Considering Variance Ratios

Figure 4 shows a horizontal bar chart of the Explained Variance Ratio (EVR) for each feature, sorted in ascending order. A few features dominate the variance, with 'Dst Port' explaining 39.14%, followed by 'Protocol' (17.02%) and 'Flow Duration' (12.59%), collectively accounting for over 68% of the variance. The remaining features, including packet length metrics, contribute less than 5% each, highlighting a clear hierarchy in feature importance.

D. Data Splitting

Once finish the aforementioned tasks, we split the dataset in half, making 90% of original data training set and 10% test set.

E. Model Classification

Image processing applications, such face recognition, have made extensive use of CNN's convolutional computation due to its strong spatial perception capabilities. During transmission, service packets created by users are divided in networks [23]. Each service packet's IP address field stands in for the traffic's geographical characteristics. In this article, we employ a CNN model to harvest traffic packets' patio-temporal characteristics, taking into account the traffic data's inherent patio-temporal properties.

A linear transformation is performed on the neural network when the dimension of input vector is larger than that of output vector. Similar to an encoder, the neural network [24], It allows for the extraction of high-dimensional features from low-dimensional spaces. By contrast, a neural network may achieve high-dimensional reconstruction of low-dimensional

characteristics in the same way as a decoder does when the output dimension is larger than the input vector dimension. The mathematical function (f*g)(n) is defined in continuous space as per to Equation (3):

$$(f * g)(n) = \int_{-\infty}^{+\infty} f(\tau)g(n-\tau)d\tau \quad (3)$$

The discrete definition is shown in Equation (4):

$$(f * g)(n) = \sum_{\tau=-\infty}^{+\infty} f(\tau)g(n-\tau) \quad (4)$$

A CNN may learn a great variety of mapping relationships between inputs and outputs; it is basically an input-to-output mapping.

F. Evaluation Metrics

To measure how well our experiment worked, we used the following five criteria: Precision, F1-Score, Accuracy, and the loss function have been studied. The parameters that make up an F1-score are accuracy, recall, and precision. The formulas for the metrics can be found in Eequations (5)-(8): By integrating the two measures, loss is a measure of the extent to which the model failed to fulfil the targets; it provides a more comprehensive view of the model's performance.

$$Acc = \frac{TP+TN}{P+N} \quad (5)$$

$$Pre = \frac{TP}{TP+FP} \quad (6)$$

$$Rec = \frac{TP}{TP+FN} \quad (7)$$

$$F1 = \frac{2\times precision\times recall}{precision+recall} \quad (8)$$

Number of instances which are properly predicted as positive is probable TP parameter of confusion matrix. Number of occurrences which are accurately predicted as negative is TN, and model successfully recognises positive events. The model gets negative situations right, where FP is the number of times it gets positive predictions wrong. Number of occurrences which are falsely predicted as negative is denoted by FN, and model predicts positive even if the actual class is negative. Although actual class is positive, model expects it to be negative.

IV. RESULTS AND DISCUSSION

A Lenovo Ideapad 500 desktop computer with Windows 10 Pro 64-bit installed was used for the research. The system's CPU was an Intel(R) Core i5-6200U, which could reach clock speeds of up to 2.40 GHz and had 8.0 GB of RAM. Table III shows performance comparison of novel CNN-based model of anomaly detection on zero-trust cloud networks. As can be seen, the model has a very high effectiveness in all the performance measures. In particular, it reaches the accuracy of 99.87, which means that it labels the vast majority of cases correctly. Values of recall and precision are 99.86 and 99.86 correspondingly, indicating that the model has a high ability to reduce false positives with at the same time establishing practically all relevant anomalies. Moreover, the F1-score of 99.87 percent validates the equal performance of the model regarding the recall and precision. All these outcomes underscore effectiveness and dependability of the suggested CNN model in providing the correct AD in zero-trust cloud architecture.

Table 3 : Performance Results of the Proposed Model for Anomaly Detection in Zero-Trust Cloud Networks

Metrics	CNN
Acc.	99.87
Pre.	99.86
Rec.	99.86
F1-Score	99.87

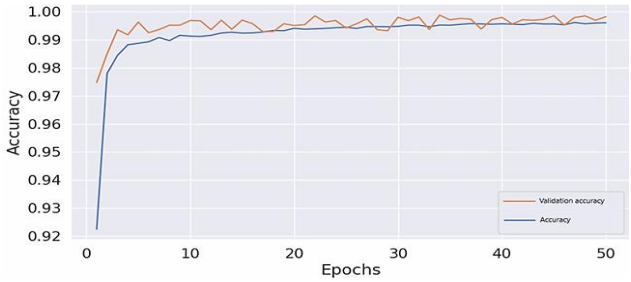

Figure 5 : Validation and Training Accuracy Curve of the CNN Model

The model's accuracy throughout validation and trainings across 50 epochs is shown in Figure 5. Both accuracies start moderately (0.92–0.97) and rise steeply within the first few epochs, surpassing 0.99. Thereafter, they stabilize with minimal fluctuations, remaining close to 1.00. Notably, with no indications of overfitting, validation accuracy typically meets or slightly surpasses training accuracy, suggesting robust generalisation.

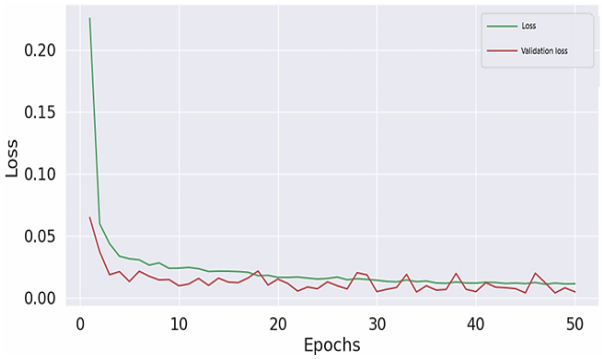

Figure 6 : Validation and Training Loss Curve of the CNN Model

Loss for validation and training during 50 epochs is displayed in Figure 6. Both begin high (training loss >0.20) and drop steeply below 0.05 within the first few epochs. They then gradually decline and stabilize near zero for the remaining epochs. Validation loss stays slightly lower than training loss, indicating effective error minimization and no signs of underfitting or overfitting.

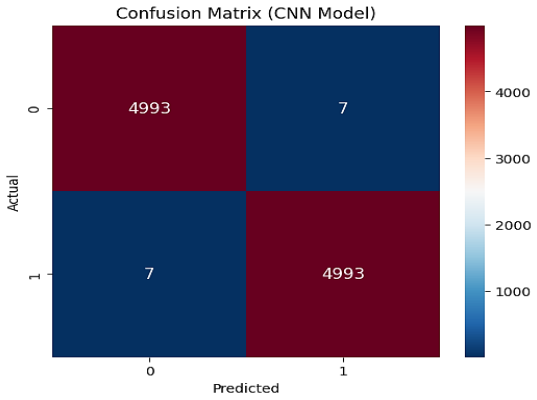

Figure 7 : Confusion Matrix of the CNN Model

Figure 7 presents the confusion matrix of CNN model for a binary classification task with classes *Positive* and *Negative*. The model demonstrates outstanding performance, with 4993 True Positives, while errors are minimal, with only 7 False Negatives. The colour intensity confirms the dominance of correctly classified instances. This highly balanced outcome indicates the CNN achieves near-perfect accuracy across both classes.

A. Comparative Analysis

In order to identify anomalies in zero-trust cloud networks, Table IV compares the suggested CNN model's performance to that of benchmarking models. Among the baseline models, Multilayer Perceptron – Particle Swarm Optimization (MLP-PSO) achieved high accuracy (95.32%) with strong precision, recall, and F1-score, while LSTM further improved performance with 98.83% accuracy. SVM model, however, performed relatively lower, with 74.7% accuracy and 80.1% F1-score. Conversely, proposed CNN model bested the rest, achieving near-perfect 99.87% accuracy and balanced recall, F1-score of 99.86–99.87, and precision, and thus exhibits better ability to detect anomalies.

Table 4 : Performance Comparison of Benchmarking Models with the Proposed Models for Anomaly Detection in Zero-Trust Cloud Networks

Models	Accuracy	Precision	Recall	F1-Score
MLP-PSO [25]	95.32	98.97	96.27	97.60
LSTM [26]	98.83	98.34	98.83	98.37
SVM [27]	74.7	86	75	80.1
CNN	99.87	99.86	99.86	99.87

The CNN-based model suggested has major benefits to the study of anomalies in the zero-trust cloud networks. The hierarchical structure makes it automatic in feature extraction, to detect more complicated patterns and finer anomalies without human supervision. The model has high generalization, does not overfit, and it has effective detection of common and rare threats. It is scalable and adaptable, which is why it is used in large-scale and dynamic environments. In general, it offers a valid and effective means of achieving changing zero-trust architectures.

V. CONCLUSION

Scouting anomaly detection is central to achieving zero-trust cloud networks since conventional solutions that rely on the perimeter approach cannot withstand advanced cyber threats. The growing density and complexity of clouds require smart and automated systems to detect unusual traffic in a network. Deep learning and machine learning-based solutions have come up as effective methods of identifying known and novel attacks with high accuracy. This paper proposes a CNN-based anomaly detector model of zero-trust cloud networks based on the use of the CSE-CIC-IDS2018 dataset. Extensive pre-processing such as outlier reduction through LOF, Z-score normalization and dimensionality reduction based on PCA was done to improve model performance. Recall, accuracy, and F1-score for suggested CNN model ranged from 99.86 to 99.87, indicating very excellent performance, which was better than the benchmark models, including MLP-PSO, LSTM, and SVM. It is highly suitable to dynamic cloud environments due to its deep hierarchical structure which enables automatic feature extraction, high generalization and detection of common and rare anomalies.

Hybrid architectures (CNN-LSTM or attention-based models) can be investigated in the future to learn the more complicated temporal patterns of the traffic. Moreover, adding online learning, adversarial testing, and edge deployment solutions may additionally complement the real-time detection features and scalability to make the security of evolving zero-trust cloud networks more robust.

VI. REFERENCES

[1] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations,” Sensors, vol. 23, no. 15, 2023, doi: 10.3390/s23156666.

[2] D. Patel, “Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity,” Tech. Int. J. Eng. Res., vol. 10, no. 6, pp. 853–858, 2023, doi: 10.56975/tijer.v10i6.158517.

[3] P. Gogoi, D. K. Bhattacharyya, B. Borah, and J. Kalita, “A Survey of Outlier Detection Methods in Network Anomaly Identification,” Comput. J., vol. 54, pp. 570–588, 2011, doi: 10.1093/comjnl/bxr026.

[4] D. Patel, “Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 454–464, Jan. 2023, doi: 10.48175/IJARSCT-11900D.

[5] V. M. L. G. Nerella, “A Database-Centric CSPM Framework for Securing Mission-Critical Cloud Workloads,” Int. J. Intell. Syst. Appl. Eng., vol. 10, no. 1, pp. 209–217, 2022.

[6] V. Verma, “Big Data and Cloud Databases Revolutionizing Business Intelligence,” TIJER, vol. 9, no. 1, pp. 48–58, 2022.

[7] S. S. Synam Neeli, “Critical Cybersecurity Strategies for Database Protection Against Cyber Attacks,” J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, Nov. 2022, doi: 0.51219/JAIMLD/sethu-sesha-synam-neeli/461.

[8] A. R. Bilipelli, “End-to-End Predictive Analytics Pipeline of Sales Forecasting in Python for Business Decision Support Systems,” Int. J. Curr. Eng. Technol., vol. 12, no. 6, pp. 819–827, 2022.

[9] W. Yeoh, M. Liu, M. Shore, and F. Jiang, “Zero trust cybersecurity: Critical success factors and A maturity assessment framework,” Comput. Secur., vol. 133, Oct. 2023, doi: 10.1016/j.cose.2023.103412.

[10] H. Kali, “The Future Of Hr Cybersecurity: Ai-Enabled Anomaly Detection In Workday Security.,” Int. J. Recent Technol. Sci. Manag., vol. 8, no. 6, 2023, doi: 10.10206/IJRTSM.2025803096.

[11] S. Srinivasan, R. Sundaram, K. Narukulla, S. Thangavel, and S. B. Venkata Naga, “Cloud-Native Microservices Architectures: Performance, Security, and Cost Optimization Strategies,” Int. J. Emerg. Trends Comput. Sci. Inf. Technol., vol. 4, no. 1, pp. 16–24, 2023, doi: 10.63282/3050-9246.ijetcsit-v4i1p103.

[12] V. Shah, “Analyzing Traffic Behavior in IoT-Cloud Systems : A Review of Analytical Frameworks,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 9, no. 3, pp. 877–885, 2023, doi: 10.32628/IJSRCSEIT.

[13] K. Arshad et al., “Deep Reinforcement Learning for Anomaly Detection: A Systematic Review,” IEEE Access, vol. 10, pp. 124017–124035, 2022, doi: 10.1109/ACCESS.2022.3224023.

[14] S. H. Haji and S. Y. Ameen, “Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques: A Review,” Asian J. Res. Comput. Sci., 2021, doi: 10.9734/ajrcos/2021/v9i230218.

[15] R. Sharma, C. A. Chan, and C. Leckie, “Probabilistic Distributed Intrusion Detection For Zero-Trust Multi-Access Edge Computing,” in NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, May 2023, pp. 1–9. doi: 10.1109/NOMS56928.2023.10154326.

[16] H. A. Hassan, E. El-Din Hemdan, M. Shokair, F. E. A. El-Samie, and W. El-Shafai, “An Efficient Attack Detection Framework in Software-Defined Networking using Intelligent Techniques,” in ICEEM 2023 - 3rd IEEE International Conference on Electronic Engineering, 2023. doi: 10.1109/ICEEM58740.2023.10319575.

[17] S. S. Khan and A. B. Mailewa, “Detecting Network Transmission Anomalies using Autoencoders-SVM Neural Network on Multi-class NSL-KDD Dataset,” in 2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023, 2023. doi: 10.1109/CCWC57344.2023.10099056.

[18] A. Vinolia, N. Kanya, and V. N. Rajavarman, "Machine Learning and Deep Learning based Intrusion Detection in Cloud Environment: A Review," in Proceedings - 5th International Conference on Smart Systems and Inventive Technology, ICSSIT 2023, 2023. doi: 10.1109/ICSSIT55814.2023.10060868.

[19] W. Yunanto and H. K. Pao, "User Behaviour Risk Evaluation in Zero Trust Architecture Environment," in 2022 IEEE 8th World Forum on Internet of Things, WF-IoT 2022, 2022. doi: 10.1109/WF-IoT54382.2022.10152197.

[20] A. Srinivasan, V. Parmar, T. Oh, J. Ryoo, and M. Viglione, "Anomaly Detection System for Smart Home using Machine Learning," in 2021 International Conference on Software Security and Assurance (ICSSA), IEEE, Nov. 2021, pp. 52–55. doi: 10.1109/ICSSA53632.2021.00018.

[21] S. Satam, P. Satam, and S. Hariri, "Multi-level Bluetooth Intrusion Detection System," in Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, 2020. doi: 10.1109/AICCSA50499.2020.9316514.

[22] P. Nskh, M. N. Varma, and R. R. Naik, "Principle component analysis based intrusion detection system using support vector machine," in 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2016, pp. 1344–1350. doi: 10.1109/RTEICT.2016.7808050.

[23] Y. Zhang, X. Chen, L. Jin, X. Wang, and D. Guo, "Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data," IEEE Access, vol. 7, pp. 37004–37016, 2019, doi: 10.1109/ACCESS.2019.2905041.

[24] H. Liu and H. Wang, "Real-Time Anomaly Detection of Network Traffic Based on CNN," Symmetry (Basel)., vol. 15, no. 6, Jun. 2023, doi: 10.3390/sym15061205.

[25] S. Alzughaibi and S. El Khediri, "A Cloud Intrusion Detection Systems Based on DNN Using Backpropagation and PSO on the CSE-CIC-IDS2018 Dataset," Appl. Sci., vol. 13, no. 4, 2023, doi: 10.3390/app13042276.

[26] Y.-C. Wang, Y.-C. Houng, H.-X. Chen, and S.-M. Tseng, "Network Anomaly Intrusion Detection Based on Deep Learning Approach," Sensors, vol. 23, no. 4, p. 2171, Feb. 2023, doi: 10.3390/s23042171.

[27] P. Lin, K. Ye, and C.-Z. Xu, Dynamic Network Anomaly Detection System by Using Deep Learning Techniques. 2019. doi: 10.1007/978-3-030-23502-4.