Identification of Anomalies via Deep Learning-Based Models for High-Dimensional Telecom Traffic Data

Henry P Cyril[1*], Shiva Kumara[2]

[1] Anna University, Chennai, India.
[2] University of Washington, Seattle, USA.

* Corresponding author. Email: henry.cyril.tech@gmail.com (H.P.C.); reachkumaras@gmail.com (S.K.)
Manuscript submitted January 13, 2026; accepted January 23, 2026; published February 25, 2026.
doi: 10.18178/JAAI.2026.4.1.24-37

Abstract: The rapid growth in size and complexity of today's telecommunication networks has created opportunities for networks to be attacked via anomalous behaviors, adversely impacting the security, reliability and performance of network services. The traditional approaches for identifying anomalies in networks (Rule-Based Anomaly Detection) do not perform as well when applied to high-dimensional, dynamically changing traffic patterns, thus limiting their applicability to real-world environments. Suggested a novel Deep Learning-based architecture for identifying traffic irregularities in telecommunications networks in order to address this issue. The framework includes a comprehensive set of data preprocessing techniques, such as Feature normalization of the data values and techniques for balancing the classes within the Data Set, that allow for the creation of unique models capable of discriminating between normal and anomalous traffic. developed and evaluated two different deep learning architectures for the problem; an Artificial Neural Network (ANN) and a 1D Convolutional Neural Networks (CNN) using the Network Traffic Anomaly Detection Dataset (Kaggle). The experimental results show that both of the models perform significantly better than traditional machine learning techniques, i.e., ANN achieved 95.27% accuracy as well as best F1-Score while the CNN detected the temporal traffic patterns. The recall values were consistently high across both architectures, indicating that both architectures are capable of detecting anomalous events reliably. Therefore, the proposed framework shows promise for the development of scalable Real-Time Telecommunication Network Anomaly Detection Systems.

Keywords: network traffic anomaly detection, deep learning, telecom security, traffic data, traffic pattern analysis

1. Introduction

The security, dependability, and functionality of the existing telecommunications infrastructures depend on anomaly detection [1]. The main aim of it is to detect abnormal behaviors, which can specify faults, degrade performance, or present a threat to security during the network operations [2]. With the scale and complexity of telecom networks increasing with large volumes of traffic, with the use of heterogeneous services, and with new communication technologies, the shortcomings of the traditional rule-based anomaly detection techniques have become more apparent [3, 4]. The anomalies in network traffic may appear in many forms, starting with harmless changes in the nature of traffic flows [5] to serious risks to security, such as Distributed Denial of Service (DDoS), loss of data, or spread of malware. Such anomalies may come with serious consequences such as loss of data integrity, poor network performance, financial losses and user trust loss [6].

As such, the in-time and precise identification of such anomalies is profound to the integrity and safety of network systems [7].

Because of the internet-based networks' and communication systems' explosive rise, information technology professionals are always challenged in tracking and securing the network infrastructures [8, 9]. Even though the currently available solutions to anomaly detection may claim a high level of theoretical performance, a number of them do not adequately classify actual network traffic in various operating environments [10, 11]. Traditional methods tend to use set thresholds and rules, which are difficult to adjust to the changing traffic trends and the shifting threat environments [12]. These techniques have serious limitations of scalability, real-time response and fidelity in handling large high-dimensional telecom data. Consequently, unanticipated network errors and anomalies left unnoticed causing disruption of services and quality of service, financial losses and severe security breach [13, 14].

The main strength of deep learning is that it can quickly process high-dimensional data and reveal relationships between variables that can be overlooked using conventional methods. Deep learning models are able to learn representative features on the raw data automatically; no manual feature engineering is needed [15, 16]. Also, their support to work within data-driven and unsupervised or semi-supervised conditions is especially useful in network environments where the availability of labeled data is scarce, and abnormal patterns and the emergence of threats can be identified effectively [17, 18]. This study develops a proposed framework for detecting abnormal network traffic via deep learning techniques in the complex telecom network space to demonstrate the improved detection performance, improved scalability, and ability to apply the framework through the use of feature learning processes. The following research contributions of this paper are:

- The proposed framework is implemented using Artificial Neural Network (ANN) and Convolutional Neural Networks (CNN).
- Data preprocessing includes class validation, scaling, and feature balancing.
- The proposed framework demonstrated the ability to accurately detect anomalies in the network traffic anomaly detection dataset in a realistic manner.
- Delivered comparative analysis to demonstrate the advantages of convolution-based models to identify new temporal patterns of traffic.

This study is organized as follows: a review of relevant literature is provided in Section 2. Section 3 gives the proposed methodology. In Section 4, the experimental design and findings are discussed. Section 5 gives a comparative analysis of the model performance and how it was discussed and how it had limitations. Lastly, Section 6 gives a review of the study's major contributions and an outline of potential future research directions.

2. Literature Review

Following the literature, the complexity and scale of current network traffic are necessitating more and more dependence on deep learning-powered anomaly detection systems to offer adaptable and real-time defenses against adaptively changing network threats and network abnormal traffic.

In this study Ijaradar *et al.* [19] provides an avenue to handle spatiotemporal complexity, through use of a GCN–LSTM–Attention (Transformer) model and Adaptive Thresholds, by only evaluating on one dataset with artificial anomalies, future studies could benefit from more realistic, naturalistic anomalies across various datasets to enhance the generalizability and robustness of this approach in real-world traffic settings [19]. Also, Luo [20], in a graph neural network-based network traffic anomaly detection framework, reports an accuracy and F1-score of 91% and 0.91 portend strength, GNN-based approach, but comparable GCN and GAT performances and excellent accuracy of small- sized nodes indicate the possibility of overfitting and inadequate consideration of different network environments [20].

A year earlier, Luo *et al.* [21] provides information on the vulnerability of models trained using deep

learning, this research does not provide detailed guidance on how to mitigate the effects of attacks on these systems thereby restricting the usefulness of this work to increase the robustness of safety critical air traffic systems [21], while Ji and Ye' study [22] is a novel method to emphasize port-level significance through attention and a two-stage architecture, which is highly precise at CICIDS-2017; but is complex and highly dependent on one dataset, making it questionable that it can be scaled and generalized to changing network traffic. Another results BP, SM and LV [23] that combines RF and CNN to perform application-level anomaly detection with a large dataset of 2,793,696 packet flows is effective and attains high accuracy, but because it is based on the specific characteristics of the organization traffic, it is not applicable to encrypted or dynamic network traffic.

The quantile-based method Alsan *et al.* [24] is an effective model of the variability and imbalance of traffic, with high accuracy (better than 90) on detection of anomalies, but its performance is very much sensitive to tolerance choices, and the definite quantile values can limit scalability to dynamically changing network conditions. The research by Zheng and Li [25] presents a robust, realistic examination of training-stage poisoning attacks, which is found to degrade MSE by 50 up to 108 times; the defense mechanisms are however tested in small scale scenarios. This Table 1 systematically compares recent deep learning–based network traffic anomaly detection approaches by highlighting their methodologies, datasets, performance, limitations, and future research directions. It clearly reveals common gaps such as limited dataset diversity, scalability challenges, and robustness issues, thereby motivating the need for more generalized and adaptive anomaly detection frameworks.

Table 1. Summary of related work for anomaly detection using AI models

Reference	Method / Model	Dataset(s) Used	Key Contributions	Performance Metrics	Limitations / Research Gaps	Future Work Directions
Ijaradar *et al.* [19]	GCN–LSTM–Attention (Transformer) with Adaptive Thresholds	Single dataset with artificial anomalies	Captures spatiotemporal dependencies in network traffic	High detection accuracy (reported)	Evaluation limited to one dataset with synthetic anomalies	Validate on multiple real-world datasets with naturally occurring anomalies to improve robustness
Luo [20]	GNN-based framework (GCN, GAT)	Network traffic dataset	Demonstrates effectiveness of graph-based anomaly detection	Accuracy: 91%, F1-Score: 0.91	Possible overfitting; limited diversity of network environments	Incorporate cross-domain datasets and regularization techniques to enhance generalization
Luo *et al.* [21]	Deep learning-based anomaly detection under adversarial attacks	Air traffic / network traffic data	Identifies vulnerabilities of DL models to poisoning and adversarial attacks	Significant performance degradation under attacks	Lack of mitigation and defense strategies	Develop robust defense mechanisms and adversarial training for safety-critical systems
Ji and Ye [22]	Attention-based two-stage architecture (port-level focus)	CICIDS-2017	High precision via port-level attention modeling	High precision (reported)	High complexity; dependence on a single dataset	Simplify architecture and evaluate across evolving and heterogeneous traffic datasets
BP, SM and LV [23]	Hybrid Random Forest + CNN	2,793,696 packet flows	Effective large-scale application-level anomaly detection	High detection accuracy	Ineffective for encrypted or dynamic traffic	Extend models to handle encrypted traffic and adaptive network behaviors
Alsan *et al.* [24]	Quantile-based anomaly detection	Network traffic dataset	Addresses traffic imbalance and variability	Accuracy > 90%	Sensitivity to tolerance and quantile selection	Introduce adaptive quantile mechanisms for dynamic traffic conditions
Zheng and Li [25]	Training-stage poisoning attack analysis and defenses	Small-scale wireless networks	Realistic assessment of poisoning attacks	MSE degradation of 50–108×	Limited scalability evaluation	Test and optimize defenses for large-scale and real-world wireless networks

2.1. Research Gaps

Existing research on identifying anomalies in network traffic indicates many drawbacks, even though they report good performance. Most of the methods studied are centred around using either just one dataset or anomalies created artificially, making it difficult to apply their results to actual environments. Models based on graph theory and the use of attention-related mechanisms have produced high results but may be subject to overfitting, and many of the models have not been validated in a variety of network conditions. Many quantitative models also require the initial selection of their parameters or have been designed for a specific type of dataset; hybrid ML-DL models are also associated with this same limitation. Moreover, studies focusing on security-related activities typically discuss the problem of being vulnerable to poisoning attacks and offer little in terms of providing scalable mechanisms for defence. These factors support the need for strong, adaptive, and scalable frameworks for detecting anomalies that have been validated on multiple realistic datasets through the use of traffic data.

3. Methodology

An summary of the network traffic anomaly detection dataset is given in this section as well as the entire workflow for implementing and implementing the framework used to identify irregularities in network flow. The method starts with importing the dataset required for detecting anomalies in network traffic. Fig. 1 shows the data preparation, DL models, and assessment steps.

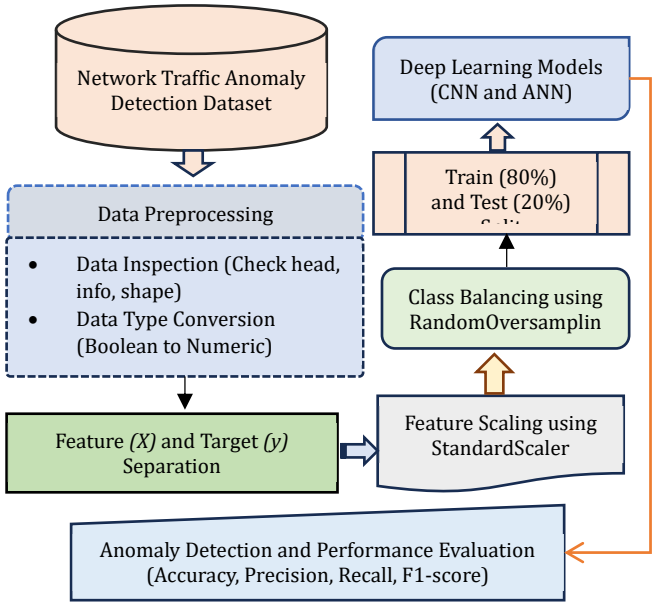

Fig. 1. A framework for detecting network traffic anomalies based on deep learning.

3.1. Dataset Collection and Preprocessing

The dataset for network traffic anomaly detection that was gathered via Kaggle consists of 1,000 records pertaining to various types of network connections, inclusive of the usual connection types and those representing network anomalies. Each of these records contains relevant information about the packet characteristics of each network connection, as well as the time and type of traffic involved for each connection; therefore, it can be used to perform supervised anomaly detection in an environment where there may be network connection anomalies.

To prepare for use with Deep Learning algorithms, all features defined as boolean were converted to

Integer Numeric type as a binary value with values between (0,1). Then a complete data type validation was performed on all features to verify whether or not the remaining features were Integer Numeric type; if not, they were removed so there would be a consistent, clean feature space, thus creating stable training, efficient training, and predictive power for the model.

The characteristics of the dataset can be better understood with the help of some graphs which indicate the distribution of class members and their inter-arrival time and graphically represent the average value of selected telecommunications features listed below.

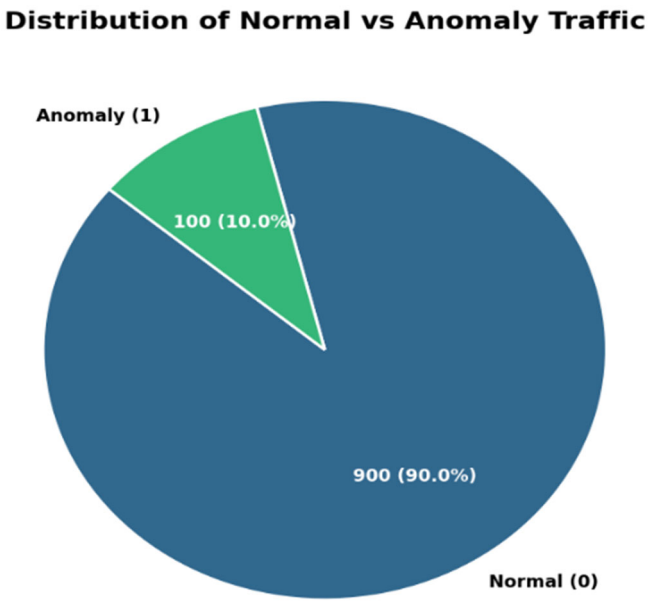

Fig. 2. Class distribution of normal and anomalous network traffic.

A class representation imbalance is present in the initial training dataset, as shown in Fig. 2. Normal traffic was represented with 900 samples (90% of the total), and anomalous traffic was represented with only 100 samples (10% of the total). Because of this, it is important to have a good class balance prior to training the model.

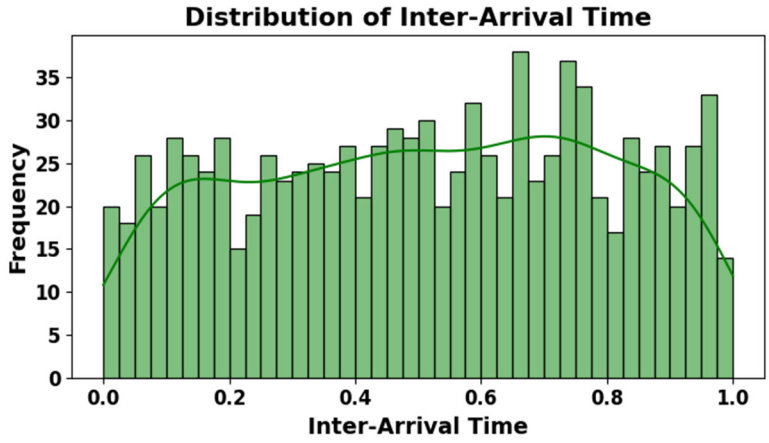

Fig. 3. Distribution of inter-arrival time.

Fig. 3 illustrates how often packets arrive over a period of time (packet inter-arrival times) and the variation and time pattern(s) associated with the data. These observations of the data distribution can assist

with understanding the normal operational characteristics of the system and recognizing traffic patterns that point to an unusual occurrence.

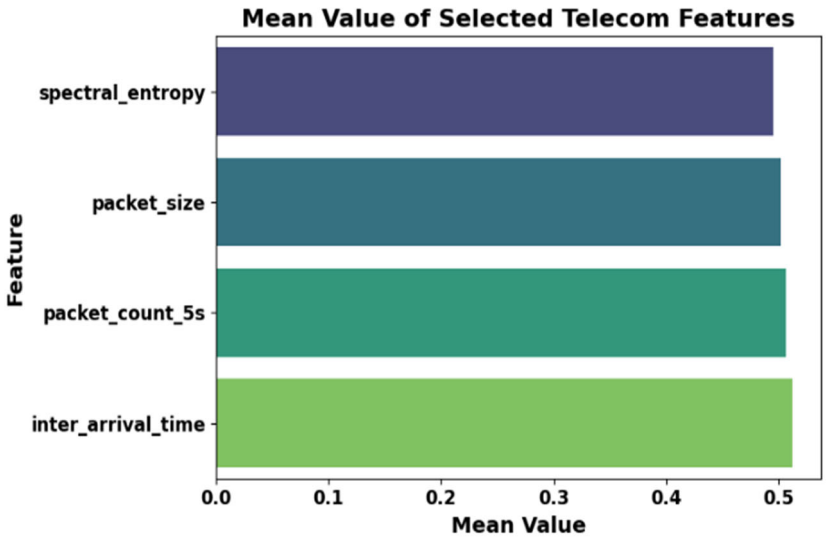

Fig. 4. Mean values of selected telecom traffic features.

In Fig. 4, the average values of several important characteristics of telecommunications (telecom) logs, such as, inter-arrival times, number of packets sent, size of packets sent, and spectral entropy, indicate the average values of these key characteristics and can be used to establish baseline traffic behaviors that allow detection of anomalous events or conditions.

3.2. Feature (X) and Target (y) Separation

The study's dataset was split into two parts: a target data set y, which includes the label variable, and a feature data set X, which comprises all of the input variables, which is the supervised learning outcome of anomalous and normal events.

3.3. Feature Scaling Using Standard Scaler

Once the features and target were separated, StandardScaler was used to normalize the feature matrix X by dividing by the unit variance after deducting the mean value. Such standardization guarantees that each of the features makes the same contribution in model training and enhances convergence and stability in learning [26]. Equation (1) for StandardScaler is as follows:

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

where the variable z represents a value that has been scaled; x represents the original value, and μ and σ are the standard deviation and mean values, accordingly, for those same feature values (also known as the data set).

3.4. Class Balancing using Random over Sampler

To address class imbalance in the dataset, Random Oversampling (ROS) was used to create additional copies of the minority class. The original data had 900 normal cases and 100 anomaly samples; following the random oversampling, the number of anomaly samples equaled that of the normal samples, increasing the overall balance between classes and allowing the deep learning algorithms the ability to learn better-defined boundaries for all cases.

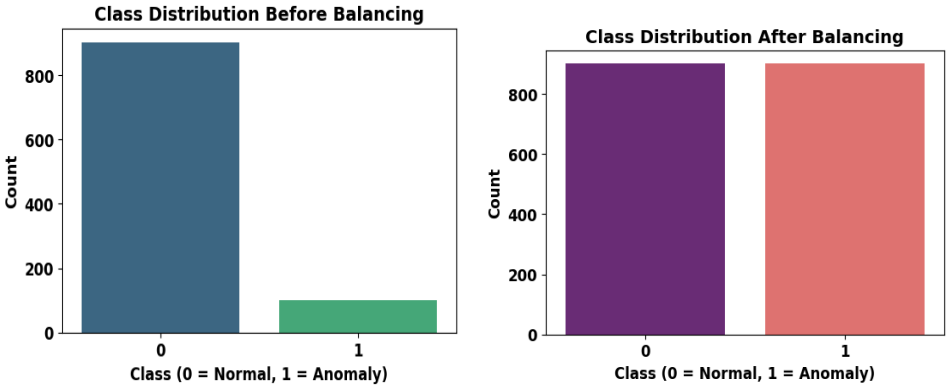

Fig. 5. Distribution of classes before and after data balancing.

The class distribution of the dataset before using Random Oversampling and after using Random Oversampling is shown in Fig. 5. Prior to balancing, the dataset was heavily imbalanced toward the normal class, with a very small number of anomaly samples. The normal class and the anomalous class are equally represented following oversampling, resulting in an even distribution of classes in the dataset, which assists in training the model fairly and helps reduce bias toward the predominant class.

3.5. Train-Test Data Partitioning

Following preprocessing, a balanced dataset was divided into training and test datasets using an 80/20 split. In addition to preserving the original distribution of the target variable's classes, stratified sampling allows for a more reliable model training process and the evaluation of new anomaly and normal examples.

3.6. Proposed Deep Learning Models for Network Traffic Anomaly Detection

In this section, the Deep Learning Network model is used for detecting anomalous network traffic. Convolutional neural networks and artificial neural networks are the model types being used in the system.

3.6.1. Convolutional neural network model

CNNs, as deep learning-based model architectures, are particularly well-suited for sequential/structured data analysis since they have the capacity to develop hierarchical feature representations automatically [27], [28]. In detecting anomalous network traffic, the ability of CNNs to model local and temporal dependence within the sequence of incoming traffic is the foundation for their proficiency in distinguishing between typical and unusual traffic.

Given an input sequence x, one-dimensional convolution operation is defined as Eq. (2):

$$c_i = f\left(\sum_{j=0}^{k-1} \omega_j \cdot x_{i+j} + b\right) \tag{2}$$

The input sequence is represented by x, the kernel has size k and is represented by ω, b is a bias term, $f(\cdot)$ is an activation function $(ReLU)$, and c_i is the feature that was selected and extracted from the input sequence at position i. Max-pooling is used to reduce dimensionality even further, by choosing the most dominant feature value, expressed as Eq. (3):

$$p = \max(c_1, c_2, \dots, c_n) \tag{3}$$

In this work, a CNN (1D) based anomaly detection system, utilizing a multi-scale inception block design featuring parallel Conv1D convolutional layers (each having kernel sizes 3, 5 & 7) is proposed as a means to capture time series traffic behavior, through dilated as well as residual convolution layers. Long-Term

Dependency Learning, as well as increased stability during training, is achieved through use of both dilated and residual convolutions. The layer structure consists of multiple convolution layers Eq. (3), which are designed to improve feature extraction and refine feature sets through the use of Max Pool as well as Dropout techniques. To reduce the risk of overfitting, there are 3 fully connected layers, each having 256, 128, & 64 neurons, respectively. The sigmoid function is used to activate the final output layer. The Adam Optimizer and binary cross-entropy loss functions were utilized to efficiently train this model, creating a model that can reliably identify abnormalities.

3.6.2. Artificial neural network model

The way the human brain functions led to the development of Artificial Neural Networks (ANNs) from a biological standpoint. Artificial Neural Networks (ANNs) are used to learn intricate, non-linear relationships between inputs and outputs [29]. ANNs use a series of connected "neurons" which take in a number of input "features" through" weighted connections," then apply some type of "activation function," to produce the output. ANNs are very powerful approximate functions, and thus can be effectively used for tasks such as classifying high-dimensional data, such as detecting attacks on networks through network traffic. The output of a neuron in a completely connected layer is calculated using Eqs. (4) and (5):

$$z = \sum_{i=1}^{n} \omega_i x_i + b \tag{4}$$

$$a = f(z) \tag{5}$$

where x_i represents the input features ω_i learnable weights, b represents the bias term, $f(\cdot)$ activation function is defined by ($ReLU$ for hidden layers, sigmoid for output layer neuron activation $h(a)$ denotes the neuron activation from hidden layer. The sigmoid function is defined as (Equation 6):

$$\hat{y} = \frac{1}{1+e^{-z}} \tag{6}$$

In this study, deep ANN were utilized as a baseline for detecting anomalies in network traffic. The ANN was composed of three fully connected layers containing ReLU-activated neurons with 256, 128, and 64 neurons and a 0.3 dropout rate to lessen the possibility of overfitting. The ANN used an output layer with a sigmoid activation function to provide binary classifications. The model was trained using binary cross-entropy loss and the Adam optimizer for 25 epochs using batch sizes of 32 and 20% of the training dataset for validation, providing the model with stable learning and the ability to generalize from unseen traffic data.

3.7. Evaluation Metrics

The confusion matrix, ROC-AUC, recall, accuracy, precision, and F1-Score were used to evaluate how well the proposed framework performs in differentiating the two classes. The formulas for calculating these metrics can be found in Eqs. (7)–(10) of this paper.

$$Accuracy = \frac{\text{TP+TN}}{\text{TP+Fp+TN+FN}} \tag{7}$$

$$Precision = \frac{\text{TP}}{\text{TP+FP}} \tag{8}$$

$$Recall = \frac{\text{TP}}{TP+FN} \tag{9}$$

$$F1 = 2 \times \frac{(precision \times recall)}{precision+recall} \tag{10}$$

Model Accuracy is the general level at which the model can make correct class predictions. Precision refers to the fraction of positive instances in comparison to all predicted positive instances. The model's ability to effectively identify real positive examples is measured by recall. The harmonic average of recall and precision is known as the F1-Score [30]. The confusion matrix's four main parts are True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN).

- **TP or True Positives ("Correct Predictions"):** Anomalies that are successfully identified as an anomaly.
- **TN or True Negatives (the opposite of "false positives"):** Normal Traffic Instances that were predicted as being normal.
- **FP or False Positives:** A predicted anomaly that is actually normal and results in calling an alert.
- **FN or False Negatives:** An anomaly predicted as a "non-anomaly", causing a missed detection.

4. Result Analysis and Discussion

The section provides the description of the implementation environment such as software tools, hardware setup, datasets, and deep learning models utilized. It also performance analysis of ANN and CNN models.

4.1. Implementation Environment and Experimental Setup

- Python 3.10 based anomaly detection platform was created using Google Colab and Windows 11 (Intel i5-6700, 8 GB RAM), which provides a multitude of libraries that can be utilized when developing machine learning models. Some examples of these libraries are TensorFlow/Keras, Scikit-Learn, Pandas, NumPy, Matplotlib, and imbalanced-learn.
- Deep Learning Models were created and tested: Deep Artificial Neural Network (DNN) and 1D Convolutional Neural Networks (CNN's) by experimenting with the dataset for network traffic anomaly detection.

4.2. Results of Proposed Models

The results of Table 2 show the effectiveness of the suggested CNN and ANN models in identifying anomalies in network traffic. ANN model shows the best overall detection capability as the accuracy is 95.27% and F1-Score is 95.49%, whereas the CNN model likewise performs well, as seen by its 94.16% accuracy and 94.48% F1-Score.

Table 2. Performance Evaluation of Proposed Deep Learning Models for Network Traffic Anomaly Detection

Models	Accuracy	Precision	Recall	F1-Score	Training Time (s)	Prediction time (s)
CNN	94.16%	89.55%	99.99%	94.48%	0.00	0.8755
ANN	95.27%	91.37%	99.98%	95.49%	9.27	0.1960

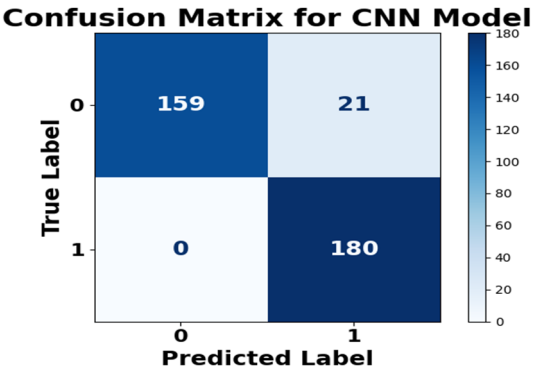

Fig. 6. Confusion matrix of the convolutional neural network.

Fig. 6 represents the results of using a CNN in terms of classifying the signals. There was a very high proportion of TP and TN with no FN, along with a low rate of false alarms. Thus, it is clear that there is great potential for identifying anomalies using this methodology.

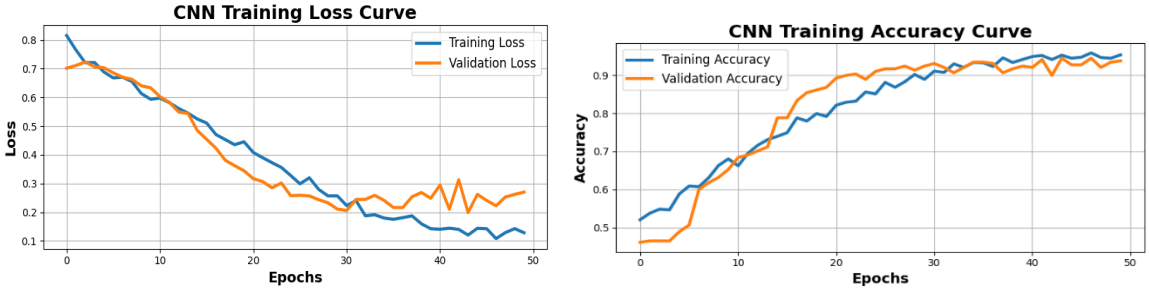

Fig. 7. CNN model training and validation accuracy and loss curves.

This graph demonstrates (Fig. 7) how well a Convolutional Neural Network converges (i.e., reduces error) when training, i.e., as the network learns, the Loss associated with the validation and training sets was steadily decreasing as well as the corresponding accuracies were increasing. Therefore, this shows that training was stable and that the model has generalized well without being affected significantly by overfitting.

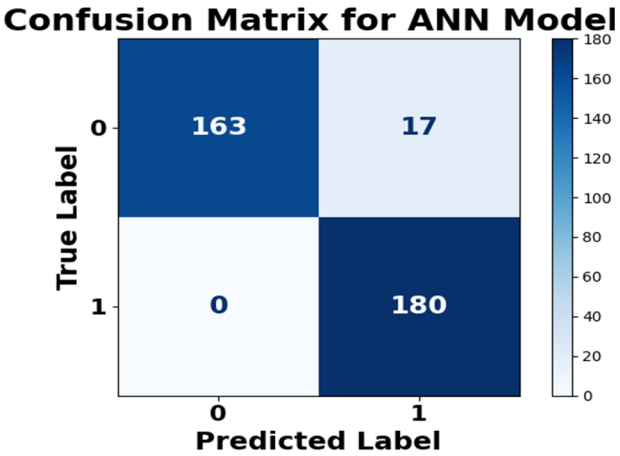

Fig. 8. Confusion matrix of the artificial neural network.

Fig. 8 shows the results of the classification in the ANN model, showing that there are many successful cases of normal and anomalous instances with zero false negatives and classification of an object. This demonstrates the model's excellent anomalous result detection and accuracy.

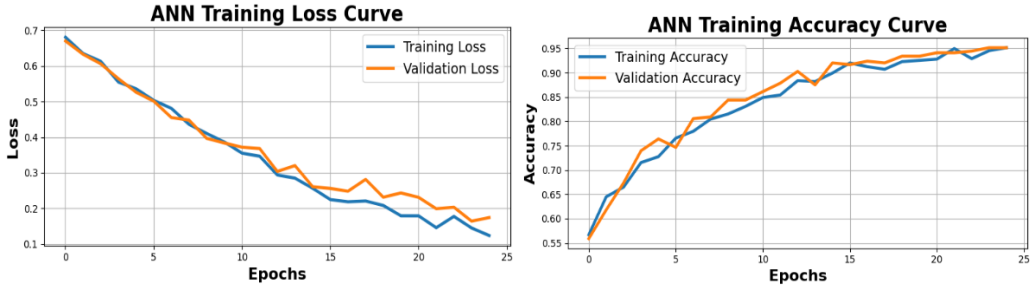

Fig. 9. Loss and accuracy curves for training and validation of the artificial neural network.

Fig. 9 shows the value depicts the learning curve of the ANN model where Training and validation loss are steadily reduced. with an equal increased accuracy that points to a successful convergence and a high generalization behavior on unknown network traffic data.

5. Comparative Analysis and Discussion

Table 3 compares the suggested Deep learning models for identifying anomalies using the Network Traffic Anomaly Detection Dataset.

Table 3. Comparison of Existing Anomaly Detection Models and the Proposed DL Framework for Network Traffic Analysis

References	Models	Accuracy	Precision	Recall	F1-Score
[31]	DANN	86.99%	87.11%	91.70%	88.23%
[32]	LR	91.20%	89.70%	90.50%	90.10%
[33]	AE	90.61%	86.83%	98.43%	92.26%
Proposed	CNN	94.16%	89.55%	99.99%	94.48%
Proposed	ANN	95.27%	91.37%	99.98%	95.49%

When comparing proposed deep learning-based anomaly detecting models and the existing machine learning models. The performance of the baseline models, the suggested CNN and ANN frameworks, and the superior outcomes of conventional models like DANN are summarized in Table 3, Logistic Regression, and Autoencoders with lower accuracy and higher F1-Scores (minimum performance is 86.99% in the DANN model). In contrast, the ANN model performs best overall with an accuracy of 95.27% and an F1-Score of 95.49%, while the CNN model has the best detection capabilities with an accuracy of 94.16% and an F1-Score of 94.48%. The high values of recall consistently suggest high recall ability, which proves the effectiveness and strength of the suggested deep learning structure to detect network traffic anomalies.

5.1. Finding and Limitations of this Study

To conclude, the study's findings show that the recommended deep learning models, i.e., the ANN and CNN are highly effective compared to the classical techniques of ML in the anomaly classification of network traffic. CNN model can be said to have a good ability to understand and record the patterns of traffic over time whereas the ANN model has got the best overall classification. Although such encouraging findings are obtained, some limitations exist. The performance is tested on one public data, which is not likely to reflect the diversity and variability of the actual telecom traffic conditions. Also, encrypted traffic, adversarial behavior factors and constraints of large-scale deployment were not investigated. The next phase of work is to test the suggested framework on various datasets, introduce robustness testing, and evaluate the work in a real-time operational network environment.

6. Conclusion and Future Work

The study offered a practical deep learning framework for identifying irregularities in network traffic using Artificial Neural Network (ANN) and Convolutional Neural Network (CNN) architectures. The framework can navigate the difficulties of a high-dimensional, complex, and dynamic The research presented a useful DL framework of detecting anomalies in the traffic of a network with an Artificial Neural Network (ANN) and a Convolutional Neural Network (CNN) structures environment in telecom traffic thanks to autonomous feature learning. The suggested models are significantly more effective than the conventional machine learning techniques, according to empirical testing of the Network Traffic Anomaly Detection Dataset. ANN has the greatest overall accuracy and F1-Score, while CNN can effectively collect temporal patterns of traffic. The high recall values are also consistent and point out the reliability of the framework in identifying an

anomalous occurrence with a low rate of false negatives. Although the above-discussed results are encouraging, the study is restricted by its assessment on one publicly available dataset and the lack of consideration of encrypted traffic, adversarial attacks, or large-scale implementation limitations. The next stage of work is the validation of the framework with various real-world data, the ability to resist adversarial and poisoning attacks, and the implementation of the models in real-time in telecommunication settings to test scalability and work performance.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

The research problem was conceptualized by Henry P. Cyril, and the framework of the deep learning-based anomaly detector was designed, the dataset was preprocessed, the ANN and CNN models were implemented, and the experimental analysis was carried out. Results interpretation and the first draft were also done by him. Shiva Kumara provided input in literature review, perfected research methodology, confirmed the experimental findings and also gave critical technical advice regarding model evaluation and comparative analysis. Findings were discussed jointly by the two authors, with the article being revised by them to make it technical and understandable, and finally, they authorized the publication. All authors had approved the final version.

Acknowledgment

The authors state that they are very grateful to the open-source research community who made publicly available datasets and tools which helped them in this study. The Network Traffic Anomaly Detection dataset provided by Kaggle is the reason to provide special thanks, as well as the creators of Python-based deep learning libraries that were used in this study.

References

[1] Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Chavez, K. G., & Rubinstein, B. (2021). Machine learning in network anomaly detection: A survey. *IEEE Access, 9*, 152379–152396. https://doi.org/10.1109/ACCESS.2021.3126834

[2] Prajapati, V. (2025). Enhancing threat intelligence and cyber defense through big data analytics: A review study. *Journal of Global Research in Mathematical Archives, 12(4)*, 1–6.

[3] Edozie, E., Shuaibu, A. N., Sadiq, B. O., & John, U. K. (2025). Artificial intelligence advances in anomaly detection for telecom networks. *Artificial Intelligence Review, 58(4)*. https://doi.org/10.1007/s10462-025-11108-x

[4] Patel, R. (2023). Automated threat detection and risk mitigation for ICS (Industrial Control Systems) employing deep learning in cybersecurity defence. *International Journal of Current Engineering and Technology, 13(6)*, 584–591. https://doi.org/10.14741/ijcet/v.13.6.11

[5] Hossain, M. S. (2024). AI-enhanced network traffic analysis: Leveraging deep learning for real-time anomaly detection and optimization. *International Journal of Research in Engineering and Science, 12(8)*, 750–764.

[6] Shah, S. B. (2025). Advancing financial security with scalable AI: Explainable machine learning models for transaction fraud detection. *Proceedings of 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICDCECE65353.2025.11034838

[7] Amrale, S. (2024). Anomaly identification in real-time for predictive analytics in IoT sensor networks using deep learning. *International Journal of Current Engineering and Technology, 14(6),* 526–532.

[8] Wang, S., Jiang, R., Wang, Z., & Zhou, Y. (2024). Deep learning-based anomaly detection and log analysis for computer networks, arXiv preprint, arXiv:2407.05639.

[9] Patel, D. (2023). Leveraging blockchain and AI framework for enhancing intrusion prevention and detection in cybersecurity. *Technix International Journal for Engineering Research, 10(6)*. https://doi.org/10.56975/tijer.v10i6.158517

[10] Thangaraju, V. (2025). Enhancing web application performance and security using AI-driven anomaly detection and optimization techniques. *International Research Journal of Innovations in Engineering and Technology, 9(3)*, 205–212. https://doi.org/10.47001/IRJIET/2025.903027

[11] Bilipelli, A. R. (2022). End-to-end predictive analytics pipeline of sales forecasting in Python for business decision support systems. *International Journal of Current Engineering and Technology, 12(6)*, 819–827.

[12] Naga, S. B. V., Thangavel, S., Kuchoor, S. K., Narukulla, N., & Yenduri, L. K. (2025). Optimizing online marketing strategies with machine learning and deep learning innovations. In A. M. George & T. K. G. (Eds.), *Impact of Digital Transformation on Business Growth and Performance* (pp. 483–512). IGI Global. https://doi.org/10.4018/979-8-3693-9783-1.ch018

[13] Shah, V. (2024). Traffic intelligence in IoT and cloud networks: Tools for monitoring, security, and optimization. *International Journal of Recent Technology Science & Management, 9(5)*. https://doi.org/10.10206/IJRTSM.2025894735

[14] Kurakula, S. R. (2025). The role of AI in transforming enterprise systems architecture for financial services modernization. *Journal of Computer Science and Technology Studies, 7(4)*, 181–186. https://doi.org/10.32996/jcsts.2025.7.4.21

[15] Kohli, M., & Chhabra, I. (2025). A comprehensive survey on techniques, challenges, evaluation metrics and applications of deep learning models for anomaly detection. *Discover Applied Sciences, 7(7)*, 784. https://doi.org/10.1007/s42452-025-07312-7

[16] Narang, S., & Gogineni, A. (2025). Zero-trust security in intrusion detection networks: An AI-powered threat detection in cloud environment. *International Journal of Scientific Research and Modern Technology, 4(5)*, 60–70. https://doi.org/10.38124/ijsrmt.v4i5.542

[17] Liso, A., Cardellicchio, A., Patruno, C., Nitti, M., Ardino, P., Stella, E., & Reno, V. (2024). A review of deep learning-based anomaly detection strategies in Industry 4.0 focused on application fields, sensing equipment, and algorithms. *IEEE Access, 12*, 93911–93923. https://doi.org/10.1109/ACCESS.2024.3424488

[18] Verma, V. (2023). Security compliance and risk management in AI-driven financial transactions. *International Journal of Engineering, Science and Mathematics, 12(7)*, 1–15.

[19] Ijaradar, J., Pape, S., Tan, C., Körner, M., & Wang, M. (2025). Data-driven anomaly detection in urban traffic data: A deep learning approach. *Proceedings of 2025 9th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)* (pp. 1–6). IEEE. https://doi.org/10.1109/MT-ITS68460.2025.11223545

[20] Luo, Y. (2025). Using graph neural networks to improve network traffic anomaly detection performance. *Proceedings of 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICDCECE65353.2025.11035232

[21] Luo, P., Wang, B., Tian, J., & Yang, Y. (2024). ADS-Bpois: Poisoning attacks against deep-learning-based air traffic ADS-B unsupervised anomaly detection models. *IEEE Internet of Things Journal, 11(23)*, 38301–38311. https://doi.org/10.1109/JIOT.2024.3446675

[22] Ji, B., & Ye, C. (2024). Network traffic anomaly detection based on port attention mechanism and ResNET-

BiLSTM-RF. *Proceedings of 2024 International Conference on Artificial Intelligence and Digital Technology (ICAIDT)* (pp. 84–88). IEEE. https://doi.org/10.1109/ICAIDT62617.2024.00026

[23] BP, V. K., SM, K., & LV, P. (2023). Deep machine learning based usage pattern and application classifier in network traffic for anomaly detection. *Proceedings of 2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS)* (pp. 50–54). IEEE. https://doi.org/10.1109/ICAECIS58353.2023.10169914

[24] Alsan, H. F., Güler, A. K., Yildiz, E., Kilinç, S., Çamlidere, B., & Arsan, T. (2023). Network traffic anomaly detection using quantile regression with tolerance. *Proceedings of 2023 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)* (pp. 300–305). IEEE. https://doi.org/10.1109/BlackSeaCom58138.2023.10299728

[25] Zheng, T., & Li, B. (2022). Poisoning attacks on deep learning based wireless traffic prediction. *Proceedings of IEEE INFOCOM 2022—IEEE Conference on Computer Communications* (pp. 660–669). IEEE. https://doi.org/10.1109/INFOCOM48880.2022.9796791

[26] Pinheiro, J. M. H., Oliveira, S. V. B. de, Silva, T. H. S., Saraiva, P. A. R., Souza, E. F. de, Godoy, R. V., Ambrosio, L. A., & Becker, M. (2025). The impact of feature scaling in machine learning: Effects on regression and classification tasks. *IEEE Access, 13*, 199903–199931. https://doi.org/10.1109/ACCESS.2025.3635541

[27] Xiang, Q., Wu, S., Wu, D., Liu, Y., & Qin, Z. (2025). Research on CNN-BiLSTM network traffic anomaly detection model based on MindSpore, arXiv preprint, arXiv:2504.21008.

[28] Prajapati, N. (2025). The role of machine learning in big data analytics: Tools, techniques, and applications. *ESP Journal of Engineering & Technology Advancements, 5(2)*, 16–22. https://doi.org/10.56472/25832646/JETA-V5I2P103

[29] Majumder, R. Q. (2025). A review of anomaly identification in finance frauds using machine learning systems. *International Journal of Advanced Research in Science, Communication and Technology, 5(10)*, 101–110. https://doi.org/10.48175/IJARSCT-25619

[30] Sinha, H. (2024). An efficient machine learning based models for anomaly detection in network traffic. *Proceedings of 2024 International Conference on Intelligent Computing and Sustainable Innovations in Technology (IC-SIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/IC-SIT63503.2024.10862888

[31] Muneer, A., Mohd, T. S., Mohamed, F. S., O. Balogun, A., & Abdul, A. I. (2022). A hybrid deep learning-based unsupervised anomaly detection in high dimensional data. *Computers, Materials & Continua, 70(3)*, 5363–5381. https://doi.org/10.32604/cmc.2022.021113

[32] Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024). Machine learning-based network anomaly detection: Design, implementation, and evaluation. *AI, 5(4)*, 2967–2983. https://doi.org/10.3390/ai5040143

[33] Assy, A. T., Mostafa, Y., El-khaleq, A. A., & Mashaly, M. (2023). Anomaly-based intrusion detection system using one-dimensional convolutional neural network. *Procedia Computer Science, 220*, 78–85. https://doi.org/10.1016/j.procs.2023.03.013

Copyright © 2026 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).