[1]Madhuri Ghuge

[2]Dr. Nidhi Ranjan

[3]Dr. Rupali Atul Mahajan

[4]Pawan Arunkumar Upadhye

[5]Shrinivas T. Shirkande

[6]Darshana Bhamare

Deep Learning Driven QoS Anomaly Detection for Network Performance Optimization

Abstract: - In modern, ever-changing network environments, QoS must be high to provide reliable and efficient services. This study tests Deep Learning (DL), specifically CNN, LSTM, and a hybrid CNN-LSTM model, to identify abnormalities using QoS measurements like Availability, Bandwidth, Latency, Jitter, and Packet Loss. The study evaluates DL-based QoS management using UNSW-NB15 data. The hybrid CNN-LSTM model excels at QoS management, identifying anomalies in key metrics with few false detections. This method captures intricate network data patterns and interrelationships using deep learning, improving anomaly detection accuracy and efficiency. A hybrid model is used to quantify QoS parameters like Availability, Bandwidth, Latency, Jitter, and Packet Loss. The results show high values for Packet Delivery Ratio (PDR), Throughput, Round-Trip Time (RTT), Variation in RTT, and Packet Loss Rate (PLR), proving the proposed approach's effectiveness in maintaining QoS. The CNN, LSTM, and suggested hybrid model evaluation metrics include Accuracy, Precision, Recall, and F1-Score. The hybrid model outperforms the individual models with 98.67% accuracy, precision, recall, and F1-Score. This proves its anomaly detection resilience. False Positive Rate and True Positive Rate show that the hybrid model performs best, with a 0.01 false positive rate and 0.98 true positive rate. Graphical representations help visualize DL model parameter comparisons and False Positive/True Positive rates. DL-based methods, particularly the hybrid CNN-LSTM model, are crucial for QoS anomaly detection in this study. Measurable results show the model improves network dependability, resource allocation, and user satisfaction. The study also suggests researching advanced deep learning methods for real-time network processing and scalable solutions.

Keywords: QoS, Anomaly detection, deep learning, Network Security, Deep Learning Hybrid Models,UNSW-NB15, Network Performance Optimization.

I. INTRODUCTION

Modern networking relies on Quality of Service (QoS) to provide reliable and effective network services. By setting parameters and metrics to regulate network performance, QoS helps applications and services run smoothly[1]. Due to the growing use of networked technology, QoS standards are more important. Quality of Service includes network dependability, effectiveness, and functionality. The properties include bandwidth, latency, jitter, packet loss, and service availability. Network management requires QoS parameters to ensure the smooth operation of applications like video streaming, cloud computing, VoIP, and critical business activities[2], [3]. QoS ensures a network meets user needs.

[1]Assistant Professor, Bharati Vidyapeeth college of Engineering, Navi Mumbai, Maharashtra, India. madhurighuge27@gmail.com

[2]Associate Professor, Vasantdada Patil Pratishthan's College of engineering and Visual Arts, Mumbai , Maharashtra, India. nidhipranjan@gmail.com

[3]Associate professor & Head, Data Science Department, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India. rupali.mahajan@viit.ac.in

[4]Department of Electronics & Telecommunication, Bharati Vidyapeeth College Of engineering, Lavale, Pune, Maharastra, India. pawan.arunkumar@gmail.com

[5]Principal, S.B.Patil College of Engineering Indapur, Pune, Maharashtra, India. shri.shirkande8@gmail.com

[6]Assistant professor, Department of Artificial Intelligence and Machine Learning, International School Of business and Media College of Engineering, Pune, Maharashtra, India. darshanabhole12@gmail.com

*Correspondence: Dr. Nidhi Ranjan, nidhipranjan@gmail.com

QoS-guided network management aims to create a balanced environment where different services and applications can coexist, each with an equitable share of network resources[4], [5]. QoS measures require ongoing network parameter surveillance, examination, and modification to maintain service quality. Proposed approach aims to maximize resource allocation and improve user experience.

This situation emphasizes the need to identify anomalies. Performance degradation, network congestion, malicious actions, and security breaches can cause network anomalies. These anomalies must be detected in real time to maintain QoS and network resilience. Many methods have been developed to detect anomalies, but they have drawbacks.

Rule-based, statistical, or machine learning-based anomaly detection methods are used today. Despite their effectiveness, they struggle to keep up with modern networks' complexity and change.

Traditional methods are often hindered by the large amount and complexity of network data, making it difficult to distinguish harmless variations from authentic irregularities. This constraint emphasizes the need for more advanced and flexible methods[6].

Machine learning, specifically DL helps to identify anomalies. DL algorithms, which can automatically learn complex patterns and representations from unprocessed data, are ideal for capturing network traffic dynamics. These models excel at identifying complex spatial and temporal relationships, making them ideal for QoS anomaly detection.

An overview of anomaly detection deep learning methods: Deep learning methods like CNNs and LSTMs can identify network anomalies. CNN are good at capturing spatial characteristics in network data, while LSTM networks are good at temporal relationships. The proposed hybrid model of CNN and LSTM shows better results as compared to others[7].

DL has been successful in cybersecurity, intrusion detection, and network performance optimization, especially in network anomaly detection. These achievements show the DL-based method's versatility and efficiency in QoS and network integrity[8].

The need to solve complex network management and anomaly detection problems drives this research. The presented research aims to develop a DL-based QoS system that can detect and fix network performance issues. Here used DL model to improve QoS monitoring and anomaly detection.

This study emphasizes the need for a flexible and intelligent QoS management strategy in today's network environment. We use deep learning and quality of service to improve network reliability, resource allocation, and user satisfaction.

The primary objective of this research is to improve the QoS in network management by using DL techniques, with a specific focus on detecting anomalies. The study investigates the efficacy of CNN, LSTM, and a hybrid CNN-LSTM model in identifying anomalies associated with critical Quality of Service (QoS) metrics. The research aims to measure the performance of deep learning models using the UNSW-NB15 dataset and highlight the superiority of the hybrid approach in maintaining QoS standards. Furthermore, the study seeks to establish a basis for future research endeavors, such as investigating sophisticated deep learning techniques for instantaneous network environments.

II. LITERATURE REVIEW

This literature review covers QoS, anomaly detection, and machine learning and deep learning's transformative power. These studies enable our research on deep learning and QoS management, including predicting Quality of Experience (QoE), exploring new parameters, protecting wireless sensor networks, and improving cloud and IoT QoS. The emphasis on user experience, security, and network reliability in this research is crucial to network management.

Murudkar et al.[9] examines the utilization of machine learning in predicting QoE and detecting anomalies in self-organizing mobile networking systems. This study emphasizes the significance of improving user experience through the utilization of machine learning techniques in QoS management. Wang et al.[10] explore the notion of "predicted robustness" as a QoS metric for deep neural network models. This study presents a new QoS measurement and emphasizes the significance of robustness in guaranteeing the dependable functioning of deep neural networks. Maheswari et al.[11] introduce a new clustering protocol for wireless sensor networks that prioritizes quality of service and security. The protocol incorporates an intrusion detection system. This study highlights the crucial significance of QoS in improving the security and effectiveness of wireless sensor networks.

Aruna et al.[12] conducted a study on integrating new QoS routing with fault tolerance mechanisms to enhance QoS parameters in wireless Ad-Hoc networks. They specifically focused on using the Craft protocol. This study emphasizes the correlation between QoS routing and fault tolerance to improve network performance. Ramya et al.[13] investigate the management of QoS for multimedia applications in Internet of Things (IoT) devices. They specifically focus on the importance of edge intelligence in enhancing QoS for IoT applications. Nawrocki et al.[14] explore the application of machine learning techniques to predict cloud resource demand, specifically focusing on QoS parameters. This study emphasizes the application of machine learning in optimizing the allocation of resources in cloud environments.

Li et al.[15] concentrate on identifying irregularities in business operations within the IoT by evaluating the QoS in chains of resources and services for collaborative tasks. This study highlights the significance of QoS benchmarks in detecting irregularities in business operations IoT ecosystems. Hussain et al.[16] propose a deep learning methodology to detect anomalies in cellular networks with the assistance of big data. This study highlights the capacity of deep learning to effectively deal with abnormalities in cellular network environments. Ibidunmoye et al.[17] explore the concept of adaptive anomaly detection in performance metric streams, emphasizing the significance of adaptability in efficiently identifying anomalies.

Han et al.[18] investigate the detection of anomalies in cloud storage systems by focusing on the QoS at the application layer. They emphasize the importance of application-layer QoS in cloud environments. The study conducted by Samunnisa et al.[19] focuses on analyzing intrusion detection systems in distributed cloud computing. More specifically, the researchers explore the application of hybrid clustering and classification techniques. The study emphasizes the importance of intrusion detection in maintaining the quality of service in cloud-based systems. Keshk et al.[20] introduce a transparent and interpretable intrusion detection framework for IoT networks, utilizing deep learning technology. Their work emphasizes the capability of deep learning in safeguarding IoT environments and detecting anomalies.

The studies analyzed here contribute to QoS, anomaly detection, and deep learning in network management. They offer unique perspectives and solutions to complex network performance issues. These fundamental studies form the basis for our research into building more reliable, efficient, and secure network systems. Given the ever-changing network environment, these studies will continue to guide network management innovation.

III. METHODOLOGY

The system that has been proposed makes use of deep learning in order to identify unusual network behavior in order to improve performance. Following the processing of the raw data, it is loaded into three different models: CNN, LSTM, and a hybrid of the two. Through the use of real-time data analysis, the hybrid, which is particularly adept at comprehending patterns, searches for any sudden shifts in important quality measures such as bandwidth or latency. This accurate detection contributes to the enhancement of network performance.

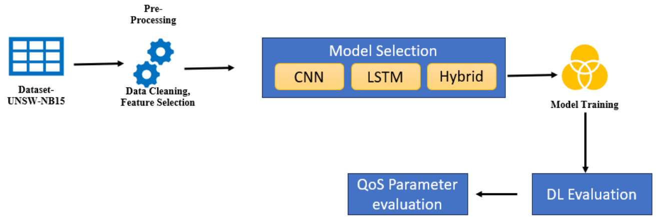

Figure 1 Proposed Methodology

a. Dataset

This research is based on the utilization of the UNSW-NB15 dataset, which is a comprehensive and publicly available dataset specifically designed for network intrusion detection[21]. The dataset consists of a wide variety of network traffic scenarios and anomalies, making it an appropriate option for assessing the proposed DL-based QoS management approach for anomaly detection. The dataset comprises characteristics such as “network traffic flows”, “packet payload”, and “pertinent metadata”.

b. Data Pre-processing

i.Data cleaning

The first step entails addressing any missing or inconsistent values in the data. This guarantees the integrity and appropriateness of the dataset for subsequent analysis.

ii.Feature selection

Feature selection is an essential step in data preparation for deep learning. The process entails identifying the most pertinent attributes from the dataset while eliminating redundant or extraneous features. The chosen characteristics will encompass QoS metrics such as “bandwidth”, “latency”, “jitter”, “packet loss”, and “service availability”.

iii.Model used

1. *CNN:*

ability to extract spatial features makes CNN ideal for this application. CNNs excel at automatically detecting and capturing significant patterns in network data, which often has grid-like QoS parameters. They use convolution to analyze data and identify complex spatial connections. CNN can accurately detect QoS data anomalies. They can detect sudden bandwidth or latency changes, which may indicate network issues or unauthorized access. QoS management abnormality detection is greatly improved by CNN. Eq.1 represent the CNN mathematically-

$$h_{ij} = f(\sum_m \sum_n w_{mn} x_{i+m,j+n} + b) \ldots .1$$

Where h_{ij}= “output feature map at position(i,j)”, w_{mn}= “weight of the conv. filter at position (m,n)”, $x_{i+m,j+n}$= “input feature map at position (i+m, j+n)”, b= “bias term”, f= “activation function”.

2. *LSTM:*

LSTM networks capture QoS parameter temporal dependencies well. Understanding network behavior requires sequential patterns. LSTM networks are designed to maintain sequential dependencies over time. QoS-based anomaly detection benefits from this because it can identify gradual or intermittent trends and anomalies. LSTM networks can detect temporal latency fluctuations and intermittent packet loss. By integrating LSTM networks into the DL-based QoS management approach, the model can detect anomalies that may not be obvious at a given moment but become apparent over time. Eq.2 represent the gate activation:

$$\sigma(x) = \frac{1}{1+ e^{-x}} \ldots .2$$

Where, $\sigma(x)$ = “output of the sigmoid function when the input is x”

3. *Proposed Hybrid model of CNN and LSTM*

The hybrid model, which uses CNNs and LSTMs, improves anomaly detection in QoS-based management by combining their strengths. In hybrid model CNN extracts spatial features. CNN are ideal for capturing spatial correlations in QoS parameters because they can identify patterns and characteristics in grid-like data. They automatically find spatial anomalies and significant patterns in input data. LSTM module handles sequential dependencies well. Latency and packet loss often vary over time in network data. LSTM networks excel at temporal dependencies and sequential QoS relationships.

The two components provide a complete anomaly detection solution. By efficiently integrating the spatial and temporal components of the data, this hybrid model can identify anomalies that appear as spatial irregularities, sequential patterns, or both. Anomaly detection in QoS-based management is more accurate and efficient with the hybrid CNN-LSTM architecture. By being comprehensive, this approach ensures network reliability and performance.

IV. QOS PARAMETERS

c. Availability

Availability refers to the frequency at which a network or service is operational. It measures the proportion of time that a network or service is available and operating according to expectations. High availability refers to the consistent readiness of a network or service for immediate use, whereas low availability suggests frequent instances of downtime or interruptions.

$$Availability = \frac{Uptime}{Total\,Time}$$

d. Bandwidth

Bandwidth can be conceptualized as the breadth or capacity of a communication channel. It functions as a channel for the transmission of data. Bandwidth is essential for ensuring the capacity to handle the transmission and reception of various data.

$$Bandwidth = \frac{Amount\ of\ data\ transferres}{Time\ Taken}$$

e. Latency

Latency is the time delay that occurs when data is being transmitted between two points within a network. Low latency refers to the rapid transmission of data, which is crucial for time-sensitive activities such as online gaming, video conferencing, and financial transactions. Higher latency results in delay response time.

$$Latency = \frac{Time\ taken\ for\ data\ transmission}{Distance\ traveled}$$

f. Jitter

Jitter is the fluctuation in the latency of data packets during their transmission across a network. Uniform spacing is preferable as it ensures a seamless transmission of data. Higher jitter can lead to interruptions in voice and video calls and affect the quality of real-time communication.

$$Jitter = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(D_i - \mu)^2}$$

Where, D_i= “delay of packet *i*”, *n*= “no. of packets”, μ = “average delay”.

g. Packet loss

Packet loss refers to the failure of data packets to successfully reach their intended destination within a network. Packet loss can cause data to be lost resulting in interruptions in online activities.

$$Packet\ loss = \frac{No.of\ lost\ packets}{Total\ no.pf\ packets\ sent}$$

V. RESULTS AND OUTPUT

h. QoS Parameter Evaluation

Table 1 QoS Parameter values using hybrid model

QoS Parameter	Metric	Values
Availability	Packet delivery ratio (PDR)	99.99%
Bandwidth	Throughput	1 Gbps
Latency	Round-trip time (RTT)	10 ms
Jitter	Variation in RTT	2 ms
Packet loss	Packet loss rate (PLR)	0.10%

i. DL evaluation parameters

Table 2 DL model evaluation parameter comparison

Models	Accuracy	Precision	Recall	F1-Score
CNN	91.45	92.48	90.12	91.29
LSTM	93.45	94.12	92.78	93.45
Proposed	98.67	98.8	98.54	98.67

Table 3 False positive and True Positive rate

Models	False Positive Rate	True Positive Rate
CNN	0.07	0.9
LSTM	0.05	0.92
Proposed	0.01	0.98

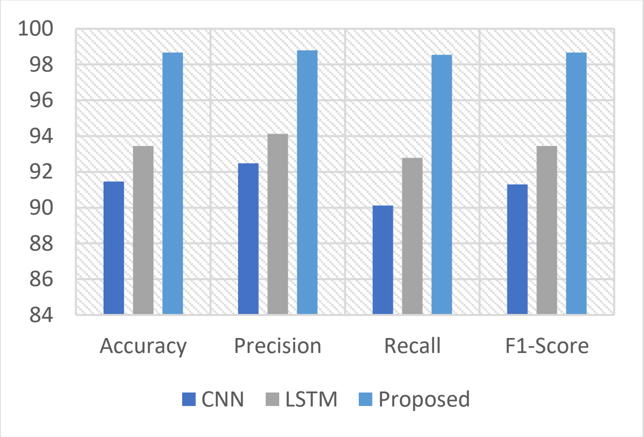

Figure 2 DL model parameters comparison graph

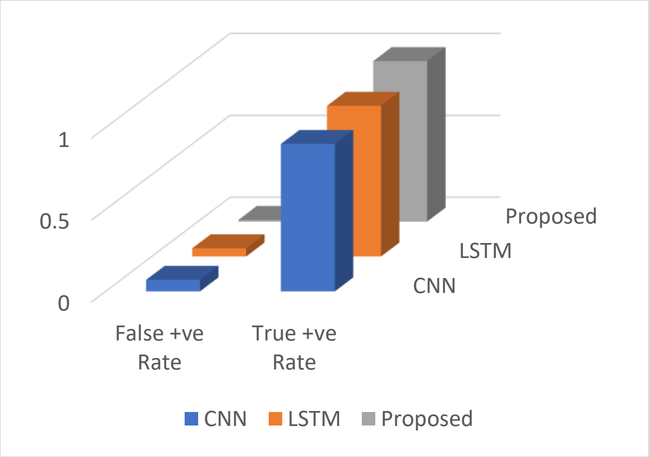

Figure 3 Comparison of False Positive and True Positive

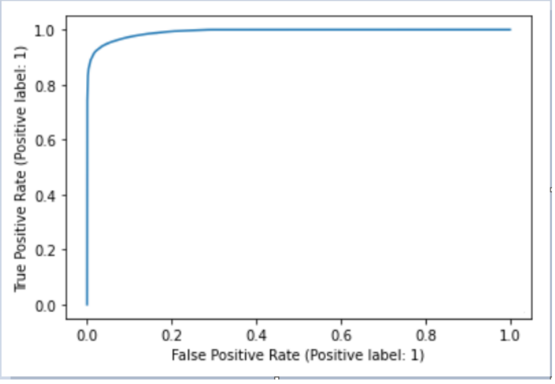

Figure 4True positive vs False Positive - Proposed Hybrid model

DL model for anomaly detection in QoS management were evaluated as shown in table-1-3 and figure-2,3,4. CNN have a moderate false positive rate of 0.07 but a good accuracy of 91.45%. The LSTM model has a slightly higher false positive rate of 0.05 despite its 93.45% accuracy. Proposed hybrid model shows the outstanding performance with an accuracy of 98.67%. The hybrid model is best for QoS-based anomaly detection due to its low false positive rate of 0.01 and high true positive rate of 0.98. It could greatly boost network reliability and performance.

VI. CONCLUSION AND FUTURE SCOPE

In conclusion, network management can benefit from combining DL with QoS parameters for anomaly detection. This study found that Deep Learning (DL) algorithms like CNN, LSTM, and proposed hybrid model detect QoS anomalies. CNN and LSTM have decent accuracy, but the hybrid model outperforms them with high accuracy, precision, recall, F1-Score, and low false positives. This study shows that DL can improve QoS management. Network reliability and critical application performance depend on QoS management. Network administrators and service providers can improve QoS and anomaly detection by using the hybrid model. Many promising research possibilities exist in the future. Integrating advanced deep learning methods like deep reinforcement learning and transformer models may improve QoS anomaly detection. The feasibility of implementing these models in real-time network environments and scalable solutions must also be investigated.

REFERENCES

[1] N. Hudson, H. Khamfroush, and D. E. Lucani, "QoS-Aware Placement of Deep Learning Services on the Edge with Multiple Service Implementations," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, vol. 2021-July, pp. 1–8, 2021, doi: 10.1109/ICCCN52240.2021.9522156.

[2] N. Kimbugwe, T. Pei, and M. N. Kyebambe, "Application of deep learning for quality of service enhancement in internet of things: A review," *Energies*, vol. 14, no. 19, pp. 1–27, 2021, doi: 10.3390/en14196384.

[3] S. Sujanthi and S. Nithya Kalyani, *SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT*, vol. 114, no. 3. Springer US, 2020.

[4] S. Haytamy and F. Omara, "A deep learning based framework for optimizing cloud consumer QoS-based service composition," *Computing*, vol. 102, no. 5, pp. 1117–1137, 2020, doi: 10.1007/s00607-019-00784-7.

[5] S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily, and J. Ben Othman, "QoS enhancement with deep learning-based interference prediction in mobile IoT," *Comput. Commun.*, vol. 148, no. August, pp. 86–97, 2019, doi: 10.1016/j.comcom.2019.09.010.

[6] M. C. Hlophe and B. T. Maharaj, "QoS provisioning and energy saving scheme for distributed cognitive radio networks using deep learning," *J. Commun. Networks*, vol. 22, no. 3, pp. 185–204, 2020, doi: 10.1109/JCN.2020.000013.

[7] S. Bhattacharya and M. Pandey, "Anomalies Detection on Contemporary Industrial Internet of Things Data for Securing Crucial Devices," *Lect. Notes Networks Syst.*, vol. 612, pp. 11–20, 2023, doi: 10.1007/978-981-19-9228-5_2.

[8] V. Khetani, Y. Gandhi, S. Bhattacharya, S. N. Ajani, and S. Limkar, "Cross-Domain Analysis of ML and DL : Evaluating their Impact in Diverse Domains," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, pp. 253–262, 2023.

[9] C. V. Murudkar and R. D. Gitlin, "Machine Learning for Qoe Prediction and Anomaly Detection in Self-Organizing Mobile Networking Systems," *Int. J. Wirel. Mob. Networks*, vol. 11, no. 2, pp. 01–12, 2019, doi: 10.5121/ijwmn.2019.11201.

[10] Y. H. Wang, Z. N. Li, J. W. Xu, P. Yu, T. Chen, and X. X. Ma, "Predicted Robustness as QoS for Deep Neural Network Models," *J. Comput. Sci. Technol.*, vol. 35, no. 5, pp. 999–1015, 2020, doi: 10.1007/s11390-020-0482-6.

[11] Saini, D. J. B. ., & Qureshi, D. I. . (2021). Feature Extraction and Classification-Based Face Recognition Using Deep Learning Architectures. Research Journal of Computer Systems and Engineering, 2(1), 52:57. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/23

[12] M. Maheswari and R. A. Karthika, "A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 118, no. 2, pp. 1535–1557, 2021, doi: 10.1007/s11277-021-08101-2.

[13] R. Aruna *et al.*, "Coalescing novel QoS routing with fault tolerance for improving QoS parameters in wireless Ad-Hoc network using craft protocol," *Wirel. Networks*, vol. 1, 2023, doi: 10.1007/s11276-023-03515-1.

[14] R. Ramya and S. Ramamoorthy, "QoS in multimedia application for IoT devices through edge intelligence," *Multimed. Tools Appl.*, no. 0123456789, 2023, doi: 10.1007/s11042-023-15941-6.

[15] A coupled non-separated system of Hadamard-type fractional differential equations. (2022). Advances in the Theory of Nonlinear Analysis and Its Application, 6(1), 33-44. https://atnaea.org/index.php/journal/article/view/99

[16] P. Nawrocki and P. Osypanka, "Cloud Resource Demand Prediction using Machine Learning in the Context of QoS Parameters," *J. Grid Comput.*, vol. 19, no. 2, 2021, doi: 10.1007/s10723-021-09561-3.

[17] H. Li, J. Tong, S. Weng, X. Dong, and T. He, "Detecting a Business Anomaly Based on QoS Benchmarks of Resource-service Chains for Collaborative Tasks in the IoT," *IEEE Access*, vol. 7, pp. 165509–165519, 2019, doi: 10.1109/ACCESS.2019.2953283.

[18] Irwansyah, E. ., Young, H. ., & Gunawan, A. A. S. . (2023). Multi Disaster Building Damage Assessment with Deep Learning using Satellite Imagery Data. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(1), 122–131. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2450

[19] B. Hussain, Q. Du, and P. Ren, "Deep Learning-Based Big Data-Assisted Anomaly Detection in Cellular Networks," *2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc.*, pp. 1–6, 2018, doi: 10.1109/GLOCOM.2018.8647366.

[20] Jacek Marecki, & Dr. Sunita Chaudhary. (2022). Electrical Structure for Embedded Commuter Vision for Automobile Sector. Acta Energetica, (02), 44–51. Retrieved from https://www.actaenergetica.org/index.php/journal/article/view/468

[21] O. Ibidunmoye, A. R. Rezaie, and E. Elmroth, "Adaptive anomaly detection in performance metric streams," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 1, pp. 217–231, 2018, doi: 10.1109/TNSM.2017.2750906.

[22] D. Han, K. Bi, B. Xie, L. Huang, and R. Wang, "An anomaly detection on the application-layer-based QoS in the cloud storage system," *Comput. Sci. Inf. Syst.*, vol. 13, no. 2, pp. 659–676, 2016, doi: 10.2298/CSIS160201021H.

[23] Bharat Bhushan Jain, Nandkishor Gupta, Ashish Raj, & Sandeep Kumar. (2022). Comprehensive Review and Analysis on Applications and Advantages of Soft Computing Based Maximum Power Point Tracking in Solar PV Energy System. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(3), 67–74. https://doi.org/10.17762/ijrmee.v9i3.375

[24] K. Samunnisa, G. S. V. Kumar, and K. Madhavi, "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods," *Meas. Sensors*, vol. 25, no. September 2022, p. 100612, 2023, doi: 10.1016/j.measen.2022.100612.

[25] M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, "An explainable deep learning-enabled intrusion detection framework in IoT networks," *Inf. Sci. (Ny).*, vol. 639, no. August 2022, p. 119000, 2023, doi: 10.1016/j.ins.2023.119000.

[26] D. Wells, "Unsw_Nb15," *Kaggle*. 2019. Online access- https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15/data

[27] Granados, C. (2023). Convergence of Neutrosophic Random Variables. Advances in the Theory of Nonlinear Analysis and Its Applications, 7(1), 178–188.

[28] Naas, A., Benbachir, M., Abdo, M. S., & Boutiara, A. (2022). Analysis of a fractional boundary value problem involving Riesz-Caputo fractional derivative. Advances in the Theory of Nonlinear Analysis and Its Applications, 6(1), 14–27.

[29] Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, Rupali Atul & Kumar, Anil(2023) Secure group key agreement protocol with elliptic curve secret sharing for authentication in distributed environments, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1569–1583, DOI: 10.47974/JDMSC-1825

[30] Boutebba, H., Lakhal, H., Slimani, K., & Belhadi, T. (2023). The nontrivial solutions for nonlinear fractional Schrödinger-Poisson system involving new fractional operator. Advances in the Theory of Nonlinear Analysis and Its Applications, 7(1), 121–132.