ISSN 2303-4521
**Periodicals of Engineering and Natural Sciences** *Original Research*
Vol. 11, No. 3, May 2023, pp.68-77

# Enhancing quality of service in IoT through deep learning techniques

**Adil M. Salman[1], Haider Rasheed Abdulshaheed[2,3], Zinah S. Jabbar [4], Ahmed Dheyaa Radhi [5] , Poh Soon JosephNg [6]**
[1] Baghdad College of Economic Sciences University, Baghdad, Iraq
[2] Computer Engineering Techniques Department, Baghdad College of Economic Sciences University, Baghdad , Iraq
[3] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad, Iraq
[4] Department of Communication Technology Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq
[5] College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq
[6] Faculty of Data Science & Information Technology, INTI International University, Persiaran Perdana BBN, 71800 Nilai, Negeri Sembilan, Malaysia

**ABSTRACT**

When evaluating an Internet of Things (IoT) platform, it is crucial to consider the quality of service (QoS) as a key criterion. With critical devices relying on IoT technology for both personal and business use, ensuring its security is paramount. However, the vast amount of data generated by IoT devices makes it challenging to manage QoS using conventional techniques, particularly when attempting to extract valuable characteristics from the data. To address this issue, we propose a dynamic-progressive deep reinforcement learning (DPDRL) technique to enhance QoS in IoT. Our approach involves collecting and preprocessing data samples before storing them in the IoT cloud and monitoring user access. We evaluate our framework using metrics such as packet loss, throughput, processing delay, and overall system data rate. Our results show that our developed framework achieved a maximum throughput of 94%, indicating its effectiveness in improving QoS. We believe that our deep learning optimization approach can be further utilized in the future to enhance QoS in IoT platforms.

**Keywords**: Quality of service (QoS), Internet of things (IoT) , Deep learning (DL), Dynamic-progressive deep reinforcement learning (DPDRL)

***Corresponding Author:***

**Poh Soon JosephNg**
Faculty of Data Science and Information Technology, INTI International University
Persiaran Perdana BBN Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
Email: joseph.ng@newinti.edu.my

## 1. Introduction

The IoT includes almost all autonomous robots, including pcs, telephones, networks, wearable technologies, controllers, and electric motors. The communication may take place over quick techniques like Wireless headphones, Enabled devices, and Bluetooth or hard cellular services like Wifi, GSM, Interaction, and internet connection like LTE, 3G, 4G, and 5G [1]. Elevated concentrations of Quality of Service must be ensured due to the widespread utilization of IoT networks, apps, and utilities in many facets of our everyday lives. The IoT greatly influences numerous parts of our everyday lives. Every other gadget has already internet access, and by 2040, it's predicted that there may be around 100 billion linked gadgets online, producing approximately 100 trillion gigabytes (GB) of information. IoT provides significant promise again for the modern intelligent environment due to the enormous quantities of data it generates [2]. The implementation of IoT on a much wider range, meanwhile, is extremely problematic, including issues regarding user privacy, environmental protection, and strategic planning, and that has a significant influence on QoS. The QoS of IoT environments and apps must be assured because numerous of our essential everyday life services rely on IoT technology [3]. IoT data may be used to enhance QoS of robotic IoT applications & services using data-driven DL techniques. IoT systems may need genuine reactions or changes after interpreting data as a method of guaranteeing excellent QoS.

Microelectronic technology, the network, and telecommunication connectivity were combined to create IoT technologies. It refers to the usage of cognitively interconnected devices to collect information from sensing devices and other physically present items which are made possible via the network [4]. They have a significant impact on customers, the neighborhood, and businesses, allowing life-improving products in a wide range of situations that fall under the categories of smart lifestyle, ecosystem, and business. In a wide range of ways, IoT technology keeps on improving user satisfaction. To address the crucial problems of available resources, power use, and protection, organizations often make use of integrated smart devices and infrastructure [5]. Due to the challenges in existing approaches, we developed a dynamic-progressive deep reinforcement learning (DPDRL). In times of high use, QoS may assist decrease congestion problems by discarding or limiting minimal loads. Additionally, QoS may significantly minimize communication delays within IoT infrastructure by employing software packet forwarding to minimize traffic in key industries of the infrastructure. Hence we enhanced QoS by proposing a dynamic-progressive deep reinforcement learning (DPDRL). Presently, IoT-based devices and systems constitute the majority. This implies that it may be harmful if such devices' QoS is weakened or fails. As a result, it must be given higher importance to guarantee the excellent QoS of such IoT-based systems. DL has been used to alter multiple Computer industries owing to its many benefits as a computation methodology. The use of DL-based techniques to assure and achieve satisfactory QoS in IoT is not entirely evident, nevertheless. Hence, we developed a dynamic-progressive deep reinforcement learning (DPDRL) for the enhancement of QoS. The remainder of this study is organized as shown in the subsequent sections. Part II presents the associated work. The methods and materials were presented in part III. P part IV explains the suggested strategy in more detail. Part V has a performance analysis segment. In part VI, the conclusion is provided.

The article [6] suggested deep learning (DL) and blockchain-empowered protection systems for intellectual fifth-generation of IoT which enables DL effectiveness for efficient information assessment processes and blockchain for user privacy. Specifically, the system would use DL for advanced information assessment activity. Through an examination of the received signal strength (RSSI) as well as the regression coefficients, the researchers in the research [7] determined the quality of the communication throughout the Time Slotted Channel Hopping (TSCH) system. The purpose is to get an understanding of the feature descriptors of such characteristics, which is necessary for selecting the optimal networks for main uses and improving the QoS of the system. The research article [8] introduced an innovative method that develops one deep learning algorithm on the infrastructure of several semi-IoT devices located all over the globe, instead of making utilize Graphics Processing Units (GPU) clusters that are placed inside a data center. The research paper [9] presented IoT devices, which are built upon deep learning sigmoid-based neural network clustering (DLSNNC) and score-based scheduling (SBS) to enhance the QoS. It is stated in the article [10] that a "mIoT-small cell-based network" may be used in a vehicle set to concentrate on public bus transport systems. Unfortunately, incorporating tiny phones in cars for mIoT poses a challenge to allocate resources due to the continuous interaction that exists among microcells. This interaction could have a detrimental influence on mobile flexibility and scalability. When it comes to WSN for the IoT, smart routing was a significant factor which required improving the QoS within the system. Moreover, a main source of resources for information exchange in Technology ad hoc networks is a significant obstacle that needs to be overcome to prevent enormous network congestion, also known as network failure, increased power loss, and inequity throughout the system, all of which can result in a decrease in base station performance and a boost in lag about the delivering of packets [11]. In the research [12], the authors presented novel holistic AI-driven IoT eHealth architecture. This work focused the "Grey Filter Bayesian Convolution Neural Network," and it is designed to lower critical service quality factors such as time and complexity while maintaining a greater degree of precision.

In the article [13], the study describes the innovative "Secure Deep Learning (SecDL)" technique that they developed for flexible spatial wireless sensor platforms to increase energy usage. In the research publication [14], the authors developed an innovative "green energy-efficient routing with DL-based anomaly detection (GEER-DLAD) approach" used for implementations. A concept that is being discussed allows IoT equipment to make use of energy efficiently in a manner that expands the channel's reach. Loss compression is the method employed in this system to minimize the amount of information that must be communicated over a system. Throughout the study [15], several difficulties and essential problems with IoT were examined, along with its design and important technology fields. Despite this, several obstacles and problems have to be fixed before the IoT can live up to its full promise. Several concerns and obstacles need to be evaluated from a variety of perspectives regarding IoT technology, including implementations, difficulties, robotics and automation, human and ecological implications, and so on. The primary purpose of this article's review is to offer a comprehensive overview from the viewpoint of both the technical as well as cultural implications of the topic.

In the research article [16], the authors undertake several analyses of how deep learning might deal without privacy protection difficulties in fifth-geneation networks, in contexts of heterogeneous "radio access networks (RANs)", extended RAN networks, and edge system layers. This is preceded by a list of important research directions and unresolved questions. Throughout the research study [17], the authors studied the combination of classification algorithms with a "Software-Defined Network (SDN) structure" to serve lag services in IoT settings. The DL with the best match is then used in a suggested advanced artificial intelligence model in the corner to retrieve an initial identified temporal information including armaments for speedy dissemination to enhance the apparent quality of service provided to the terminal [18]. The "Session Initiation Protocol," sometimes known as "SIP," is one potential foundation for such collaboration. On the other hand, because of its straightforward nature, the technique is susceptible to a wide variety of web-based assaults, including "distributed denial of service (DDoS)" and security breaches. This is suggested to use a DL-based paradigm used in the detection and mitigation of DDoS attacks in SIP-based networks [19]. In the research [20], inter-node cooperation in a spectrum-sensing framework is considered. The exponential increase of IoT fields like ubiquitous computing and Smart manufacturing must have resulted in a rise in the growth of mobile transmission capacity, which has in turn motivated the fast evolution of new boosting spectrum efficiency, especially for new wireless cellular networks. This expansion is a direct result of the exponential deployment of IoT systems.

## 2. Methods

When service providers modify system parameters to give different levels of service to respective clients, this is referred to as QoS. Qos refers to a system's capacity to provide applications with higher or more pertinent services. QoS may assist in lowering traffic load. Dynamic resource management and administration are supervised by QoS. Additionally, QoS establishes limitations and order of importance for various information types that move as broadband congestion among IP networks. The working model of the suggested technique can be seen in Figure 1.

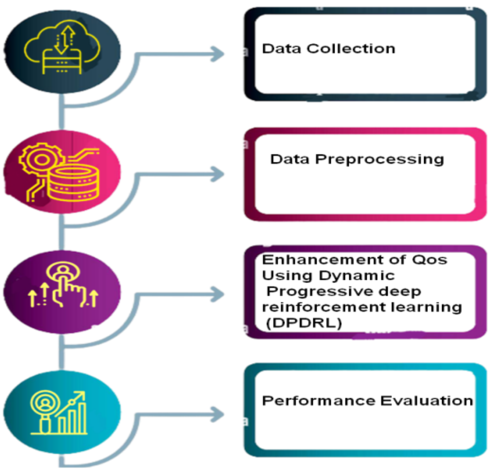


Figure 1. The working model of the proposed approach

### 2.1 Samples of data collection

The intended healthcare system gathers its information from the following two relevant data streams: Patients' routine health tracking is used to acquire the clinical information that is obtained from patient populations. Such data are first sent to associate distant portal units via Wifi or Bluetooth, and again they are sent to the cloud data centre, in which the data are preprocessed and sickness detection is performed. Some other sources of data collection are known as digital healthcare records, and it includes the individual participant's health history, evaluation statistics, and detailed patient statistics that are saved in a cloud platform. These analyses provide useful information regarding disease estimation and providing insights from healthcare experts [21-30].

### 2.2 B. Data normalization for QoS

Every level of qualitative data is distinct. For illustration, the term of expense may be millions whereas the term of processing time could be microseconds. To order to normalize such data into a single system, normalization of QoS data is required. Standardizing variables between 0 and 1 is a well-liked approach for normalization. The standardized quantities of qualitative data serve as the foundation for all subsequent computations. Two categories of QoS data are presented here:

- Utility protocol: greater value equals the better caliber
- Expense considerations: poorer performance as value increases

The following equation (1) and (2) was employed to normalize QoS data.

$$b'jk = \frac{max(bk)-bjk}{max(bk)-min(bk)}\ max(bk)! = min(bk) \qquad (1)$$

Where $b'jk = 1;\ max(bk) = min(bk)$

$$b'jk = \frac{bjk-max(bk)}{max(bk)-min(bk)}\ max(bk)!\ = min(bk) \qquad (2)$$

Where $b'jk = 1;\ max(bk) = min(bk)$

### 2.3 dynamic-progressive deep reinforcement learning (DPDRL)

Throughout this section, we briefly go to the general structure of the DPDRL we've developed before entering its specific algorithms. Figure 2 represents the DPDRL layout. The sensor, control, agent, and data layers are the basic divisions of the system [31-34].

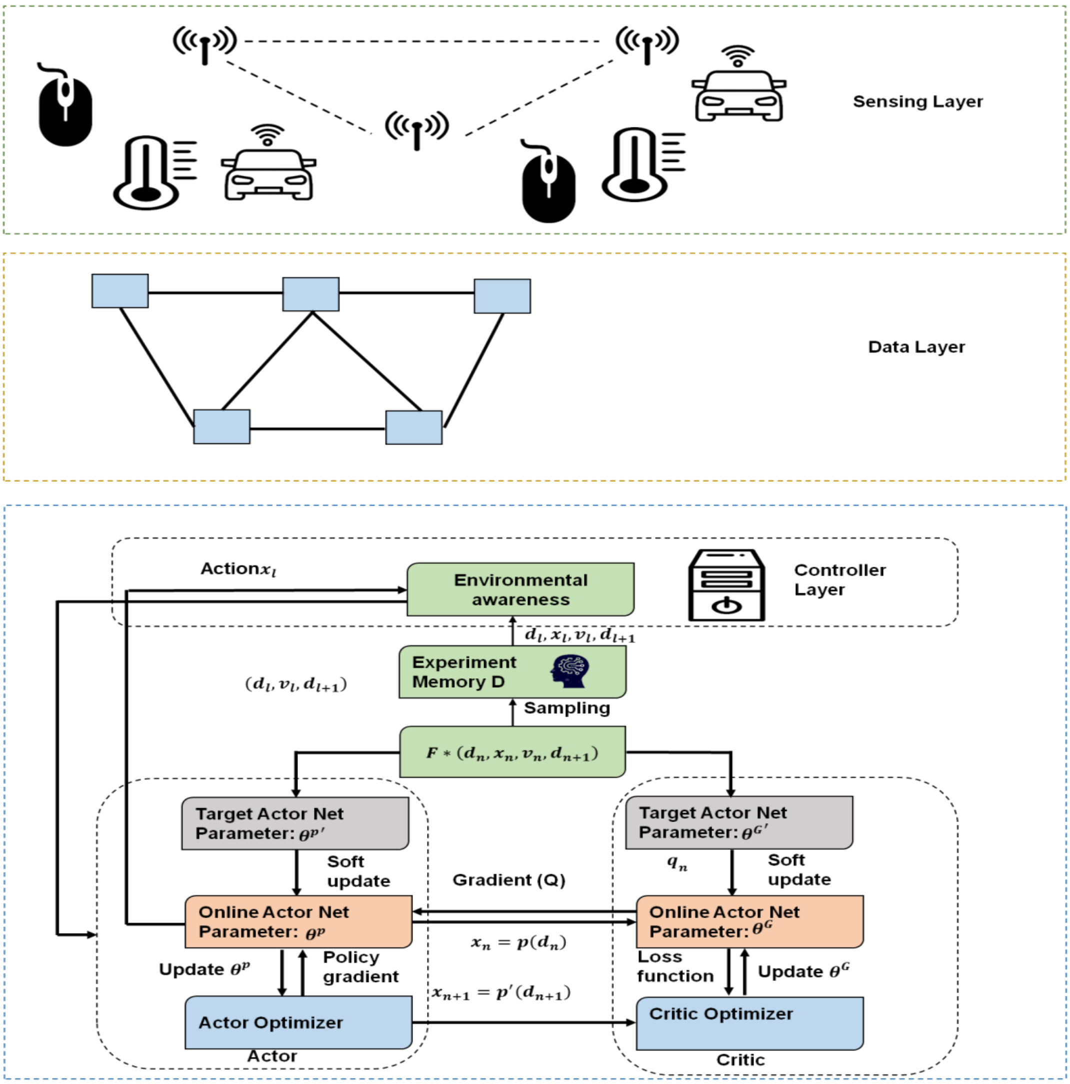


Figure 2. Layout of DPDRL

### 2.3.1 Mechanism of DPDRL layout

***A. Sensor layer***

The DPDRL design's sensor unit, which effectively accommodates a variety of wearable sensors linked via a wireless sensor network, is the foundation of the system. Information creation comes via devices, which are the fundamental part of the sensor layer.

***B. Control layer***

This layer controls routing condition transition signals along with the network's interior transfer route and the creation of a boundary access route. This layer modifies the system shifting and forwarding route in response to modifications in the network's status. Therefore, by the central power of the controllers, the system may remain in a condition of regular functioning.

***C. Data layer***

Most certain components in the data layer switch with Open Flow support. The Open flow protocol transition, which serves as the system's fundamental sending component, can only conduct forward choices by the flowing rules given by the controllers. The network model is always in charge of providing data and service statuses on the system.

***D. Agent layer***

DPDRL installed in-plane is comparable to the web application in an operating system and serves as the service's central processing unit. Through the operator's broader perspective, DPDRL can understand the network infrastructure setting. Therefore, it yields an associated forwarding strategy, assesses the program's quality after when the pathway is followed to evaluate the satisfaction achieved by the strategy, and thereafter makes adjustments to the scheme's criteria to attain greater satisfaction results. An estimated optimum forwarding plan for the network protocol may be provided by the automated tool after several periods of training utilizing previous contextual information.

### 2.3.2 Characteristics of DPDRL

In genuine internet circumstances, the reliability of the connections and the switching nodes' abilities would fluctuate while the attacks take place. Using a standard routing system to give a protected routing mechanism derived from a real distributed system is often not possible. By engaging only with context, reinforcement learning is a technique for maximizing the benefits of active learning. As a result, we design the safe routing optimization issue using deep reinforcement learning. The phases, events, and payoff values in the DPDRL must be defined to allow the DRL operator to optimize routing. The phases, events, and payoff values are defined in equations (3), (4), and (5). The working for DPDRL is presented in algorithm 1.

$$s(t_s) = \begin{bmatrix} [\Upsilon_{w_1}(t_s), \Upsilon_{w_2}(t_s), \ldots . \Upsilon_{w_p}(t_s), \\ \mathrm{Z}_{w_1}(t_s), \mathrm{Z}_{w_2}(t_s), \ldots\ \mathrm{Z}_{w_p}(t_s), \\ \mathrm{m}_{w_1}(t_s), \mathrm{m}_{w_2}(t_s), \ldots \mathrm{m}_{w_p}(t_s)] \end{bmatrix} \tag{3}$$

Here $\mathrm{Z}_{w_j} = \frac{\mathrm{A}_{w_j}(t_s)}{\mathrm{A}_{w_j}}$, $\mathrm{A}_{w_j}$ is the dimension of the flow entry in the switching network $w_j$ , *and* $\mathrm{A}_{w_j}(t_s)$ seems to be the number of flow entries utilized by the switching network $w_j$ with in time interval $t_s$.

$$l(t) = \left[l_{w_1}^{avail}(t_s), l_{w_2}^{avail}(t_s r), \ldots \ldots l_{w_p}^{avail}(t_s r)\right] \tag{4}$$

$$T(r) = \frac{1}{|F|} \sum_{j \epsilon F} \left(\alpha T_{w_j}^{attack}(t_s) + \beta T_{w_j}^{qos}(t_s)\right) \tag{5}$$

**Algorithm 1: DPDRL**

1. **for** occurance = 1 to P **do**
2. **for** r = 1 to T **do**
3. Generate a little group of F transformation randomly $\left(q(r), l(r), t(r), q(r+1)\right)$ From R
4. Put $n(r) = t(r) + \gamma S' \left(q(r+1)\mu' \left(k(r+1) \middle| \theta^{s'}\right) \middle| \theta^{s'}\right)$.
5. Modify critic by reducing the loss $A(\theta) = \frac{1}{Y} \sum_r \left(n(t) - S(q(r), l(r)|\theta^s)\right)^2$
6. Modify actor policy by generated policy gradient:

$\frac{1}{Y}\sum_j \nabla_l S(q,l|\theta^s)\big|q=q(r), l=\mu\big(q(r)\big)\nabla_{\theta\mu}\mu(q|\theta^\mu)\big|q(r)$

7. Modify the resultant networks: $\theta^{S'} \leftarrow R^{\theta^S}+(1-R)\theta^{S'}, R^{\theta^S}+(1-R)\theta^{S'}$

**8.** end **for**

**9.** end **for**

## 3. Results and discussion

The amount of value the service provides to the user determines QoS. We consider four primary characteristics to assess the effectiveness of the QoS: throughput, processing delay, packet loss, and overall system data rate. When assessing the networks, these indicators are crucial, particularly when considering the effects of the attack. The existing approaches are "Low-Power Wide-Area Networks (LPWANs), distributed coordination function (DCF), Evolutionary Gateway-based Load-Balanced Routing (E-GLBR) algorithm, and Hybrid Moth Flame Optimization (HMFO)". The ratio of the maximum number of packets to the running time is measured using throughput. The data is transferred via packets. The central server that sends a significant amount of data has the greatest efficiency. Depending upon transferred packets, overall capacity is calculated. The outcomes of comparing the throughput of the developed approach with those of the current techniques are shown in Figure 3. Comparing the presented method with the other methods currently in use, it is discovered to have a higher throughput. While the suggested system obtained 94% of throughput, the current approaches have obtained throughput of 63%, 55%, 84%, and 76%. Processing delay is the amount of time it requires for networks to evaluate a data stream in a network that utilizes packet switching. A significant contributor to network slowness is processing delay. Figure 4 shows a comparison of processing delays. The suggested technique has 53% latency, which tends to indicate higher system performance. Data packets that have been transmitted are unable to arrive at their destination this is known as packet loss. All forms of electronic communication may have observable outcome difficulties as a result of this. The packet loss comparison is demonstrated in Figure 5. Packet losses for the current approaches are 88%, 65%, 74%, and 90%, accordingly. The suggested method achieved 50% for the loss of data packets. Overall system data rate is defined as the total transmission data rate that is sent through a server in a certain period of time. It describes the speed with which data is transferred between peripherals, or between a network and output devices. In figure 6, a comparison of data rates was seen. The current approaches each have a modest system rate of 55%, 75%, 65%, and 85%. The data rate for the suggested method is 97%.

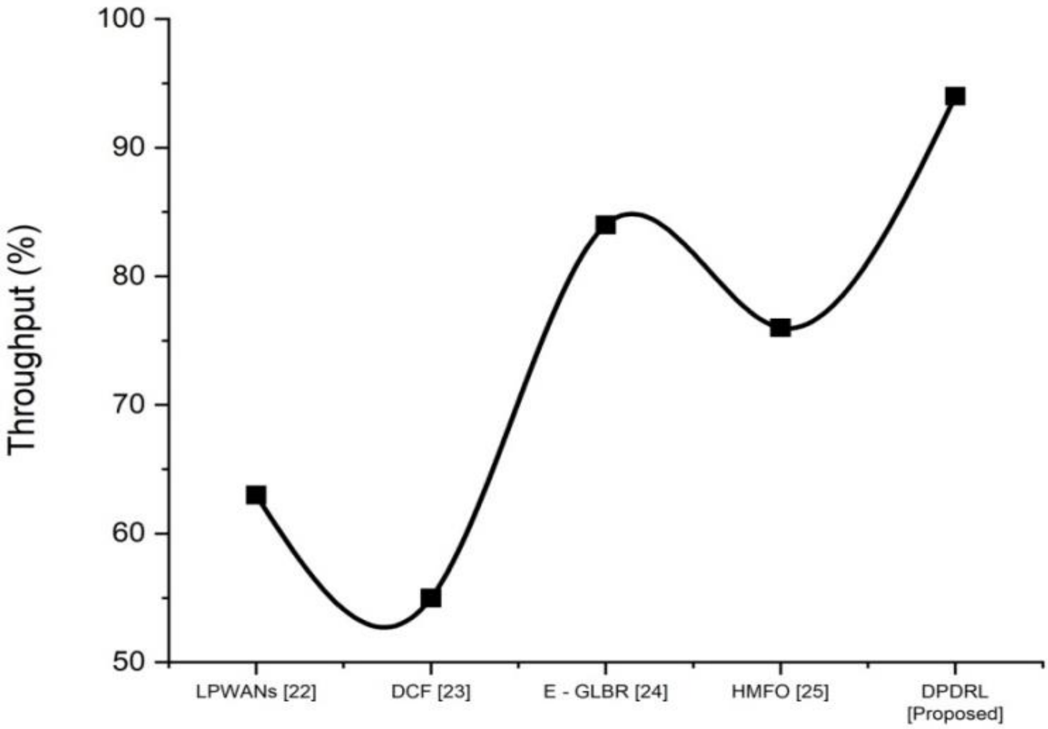


Figure 3. Statistical analysis of throughput

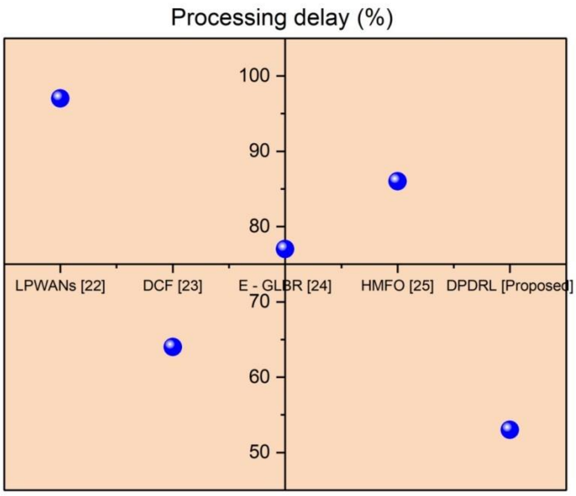


Figure 4. Statistical analysis of processing delay

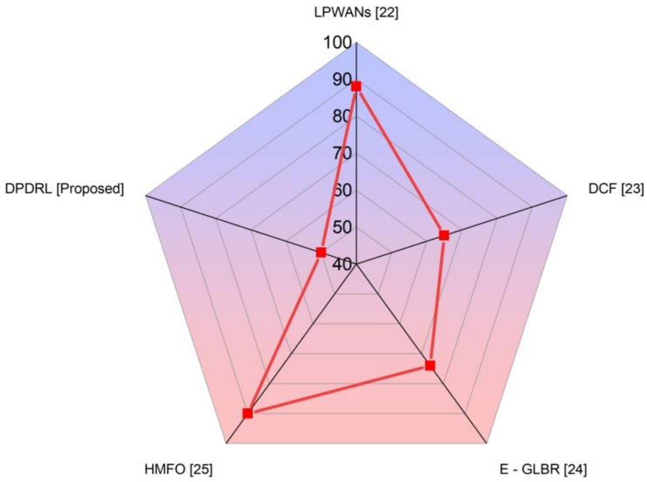


Figure 5. Statistical analysis of packet loss

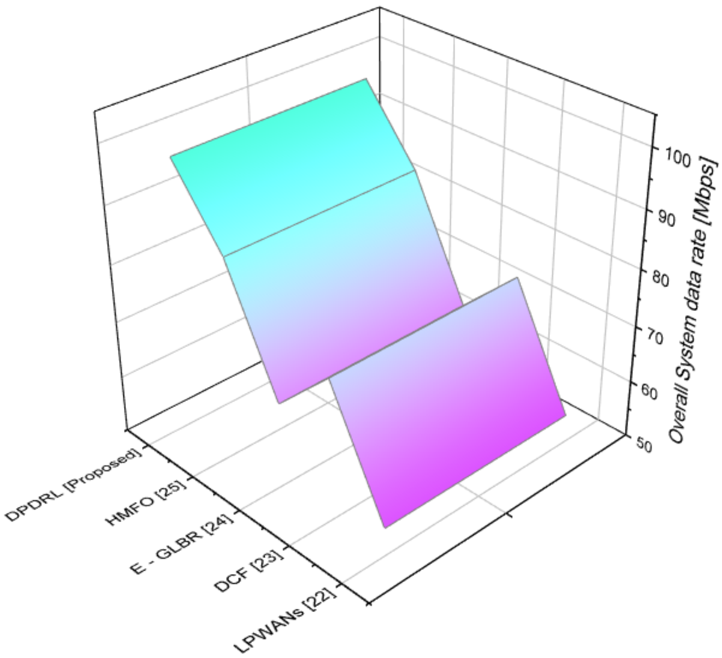


Figure 6. Statistical analysis of overall system data rate

## 4. Conclusion

Quality of Service (QoS) is a collection of services that operate on networks to ensure that the highest traffic and services may be reliably carried even when the network's capacity is constrained. The duration of time it requires for data or a transaction to be delivered and gained is known as network congestion. In this study, we created a dynamic progressive deep reinforcement learning (DPDRL) system to monitor user access and improve the QoS. The QoS data have undergone normalization. By comparing the suggested approach with currently used approaches, efficacy is examined. The throughput of the suggested strategy, in contrast, has reached 99% for enhanced quality. We will employ advanced generative adversarial networks (AGAN) in research directions to enhance the QoS needs of Software-Defined Networking (SDN)-IoT routing.

**Acknowledgements**

The authors are grateful to the Iraqi Ministry of Higher Education and Scientific Research (MOHESR) for technically supporting the current research.

**Declaration of competing interest**

The researchers certify that none of the information described in this research is subject to any known financial or non-financial competing priorities.

**Funding information**

No financial institution provided funds for the completion of this study.

**References**

[1] 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, p. 6384, Oct. 2021, doi: 10.3390/en14196384.

[2] H.-H. Liu and H.-Y. Wei, “5G NR Multicast and Broadcast QoS Enhancement With Flexible Service Continuity Configuration,” IEEE Transactions on Broadcasting, vol. 68, no. 3, pp. 689–703, Sep. 2022, doi: 10.1109/tbc.2022.3173173.

[3] K. Cao et al., “Enhancing Physical Layer Security for IoT with Non-Orthogonal Multiple Access Assisted Semi-Grant-Free Transmission,” IEEE Internet of Things Journal, pp. 1–1, 2022, doi: 10.1109/jiot.2022.3193189.

[4] M. Ali, A. Ngadi, and R. Sham, “Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle , Based on the ACO Approach,” sensors, vol. 23, no. 3, 2023.

[5] Y. Niu, I. A. M. Al Sayed, A. R. Ali, I. Al Barazanchi, and P. S. Josephng, “Research on fault adaptive fault tolerant control of distributed wind solar hybrid generator,” Bull. Electr. Eng. Informatics, vol. 12, no. 2, pp. 1029–1040, 2023, doi: 10.11591/eei.v12i2.4242.

[6] I. Al Barazanchi, H. R. Abdulshaheed, and A. Shibghatullah, “The Communication Technologies in WBAN,” Int. J. Adv. Sci. Technol., vol. 28, no. 8, pp. 543–549, 2019.

[7] Al Barazanchi, S. A. Sahy, and Z. A. Jaaz, “Traffic Management with Deployment of Li-Fi Technology,” J. Phys. Conf. Ser., vol. 1804, no. 012141, 2021, doi: 10.1088/1742-6596/1804/1/012141.

[8] S. Q. Salih, “A New Training Method Based on Black Hole Algorithm for Convolutional Neural Network,” J. Southwest Jiaotong Univ., vol. 54, no. 3, pp. 1–10, 2019, doi: 10.1002/9783527678679.dg01121.

[9] Y. Niu, S. I. Kadhem, I. A. M. Al Sayed, Z. A. Jaaz, H. M. Gheni, and I. Al Barazanchi, “Energy-Saving Analysis of Wireless Body Area Network Based on Structural Analysis,” in 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Jun. 2022, pp. 1–6, doi: 10.1109/HORA55278.2022.9799972.

[10] S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily, and J. Ben Othman, “QoS enhancement with deep learning-based interference prediction in mobile IoT,” Computer Communications, vol. 148, pp. 86–97, Dec. 2019, doi: 10.1016/j.comcom.2019.09.010.

[11] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy, and A. Kannan, “Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT,” Computer Networks, vol. 151, pp. 211–223, Mar. 2019, doi: 10.1016/j.comnet.2019.01.024.

[12] R. Patan, G. S. Pradeep Ghantasala, R. Sekaran, D. Gupta, and M. Ramachandran, “Smart healthcare and quality of service in IoT using grey filter convolutional based cyber physical system,” Sustainable Cities and Society, vol. 59, p. 102141, Aug. 2020, doi: 10.1016/j.scs.2020.102141.
[13] S. Sujanthi and S. Nithya Kalyani, “SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT,” Wireless Personal Communications, vol. 114, no. 3, pp. 2135–2169, Jun. 2020, doi: 10.1007/s11277-020-07469-x.
[14] L. Lydia, A. A. Jovith, A. F. S. Devaraj, C. Seo, and G. P. Joshi, “Green Energy Efficient Routing with Deep Learning Based Anomaly Detection for Internet of Things (IoT) Communications,” Mathematics, vol. 9, no. 5, p. 500, Mar. 2021, doi: 10.3390/math9050500.
[15] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” Journal of Big Data, vol. 6, no. 1, Dec. 2019, doi: 10.1186/s40537-019-0268-2.
[16] Y. Wu, Y. Ma, H.-N. Dai, and H. Wang, “Deep learning for privacy preservation in autonomous moving platforms enhanced 5G heterogeneous networks,” Computer Networks, vol. 185, p. 107743, Feb. 2021, doi: 10.1016/j.comnet.2020.107743.
[17] S. Q. Salih, A. A. Alsewari, and Z. M. Yaseen, “Pressure Vessel Design Simulation: Implementing of Multi-Swarm Particle Swarm Optimization,” Proc. 2019 8th Int. Conf. Softw. Comput. Appl., pp. 120–124, 2019, doi: 10.1145/3316615.3316643
[18] T. Vaiyapuri, E. L. Lydia, M. Y. Sikkandar, V. G. Diaz, I. V. Pustokhina, and D. A. Pustokhin, “Internet of Things and Deep Learning Enabled Elderly Fall Detection Model for Smart Homecare,” IEEE Access, vol. 9, pp. 113879–113888, 2021, doi: 10.1109/access.2021.3094243.
[19] N. Mahajan, A. Chauhan, H. Kumar, S. Kaushal, and A. K. Sangaiah, “A Deep Learning Approach to Detection and Mitigation of Distributed Denial of Service Attacks in High Availability Intelligent Transport Systems,” Mobile Networks and Applications, vol. 27, no. 4, pp. 1423–1443, Apr. 2022, doi: 10.1007/s11036-022-01973-z.
[20] Z. A. Jaaz, S. S. Oleiwi, S. A. Sahy, and I. Albarazanchi, “Database techniques for resilient network monitoring and inspection,” TELKOMNIKA Telecommun. Comput. Electron. Control, vol. 18, no. 5, pp. 2412–2420, 2020, doi: 10.12928/TELKOMNIKA.v18i5.14305.
[21] T. Hai et al., “DependData: Data collection dependability through three-layer decision-making in BSNs for healthcare monitoring,” Inf. Fusion, vol. 62, pp. 32–46, Oct. 2020, doi: 10.1016/j.inffus.2020.03.004.
[22] S. Q. Salih et al., “Integrative stochastic model standardization with genetic algorithm for rainfall pattern forecasting in tropical and semi-arid environments,” Hydrol. Sci. J., vol. 65, no. 7, pp. 1145–1157, May 2020, doi: 10.1080/02626667.2020.1734813.
[23] A. Malik et al., “Pan Evaporation Estimation in Uttarakhand and Uttar Pradesh States, India: Validity of an Integrative Data Intelligence Model,” Atmosphere (Basel)., vol. 11, no. 6, p. 553, May 2020, doi: 10.3390/atmos11060553.
[24] J. Li et al., “Internet of things assisted condition-based support for smart manufacturing industry using learning technique,” Comput. Intell., vol. 36, no. 4, pp. 1737–1754, 2020, doi: 10.1111/coin.12319.
[25] S. Q. Salih, “A New Training Method Based on Black Hole Algorithm for Convolutional Neural Network,” J. Southwest Jiaotong Univ., vol. 54, no. 3, pp. 1–10, 2019, doi: 10.1002/9783527678679.dg01121.
[26] H. Tao, S. M. Awadh, S. Q. Salih, S. S. Shafik, and Z. M. Yaseen, “Integration of extreme gradient boosting feature selection approach with machine learning models: application of weather relative humidity prediction,” Neural Comput. Appl., 2022, doi: 10.1007/s00521-021-06362-3.
[27] A. Malik, A. Kumar, O. Kisi, N. Khan, S. Q. Salih, and Z. M. Yaseen, “Analysis of dry and wet climate characteristics at Uttarakhand (India) using effective drought index,” Nat. Hazards, 2021, doi: 10.1007/s11069-020-04370-5.
[28] H. Tao et al., “Training and Testing Data Division Influence on Hybrid Machine Learning Model Process: Application of River Flow Forecasting,” Complexity, vol. 2020, pp. 1–22, Oct. 2020, doi: 10.1155/2020/8844367.
[29] B. Karimi, P. Mohammadi, H. Sanikhani, S. Q. Salih, and Z. M. Yaseen, “Modeling wetted areas of moisture bulb for drip irrigation systems: An enhanced empirical model and artificial neural network,” Comput. Electron. Agric., 2020, doi: 10.1016/j.compag.2020.105767.

[30] M. H. Ali, A. Ibrahim, H. Wahbah, and I. Al_Barazanchi, "Survey on encode biometric data for transmission in wireless communication networks," Period. Eng. Nat. Sci., vol. 9, no. 4, pp. 1038–1055, 2021, doi: 10.21533/pen.v9i4.2570.
[31] F. Cui, S. Q. Salih, B. Choubin, S. K. Bhagat, P. Samui, and Z. M. Yaseen, "Newly explored machine learning model for river flow time series forecasting at Mary River, Australia," Environ. Monit. Assess., 2020, doi: 10.1007/s10661-020-08724-1.
[32] T. Hai et al., "DependData: Data collection dependability through three-layer decision-making in BSNs for healthcare monitoring," Inf. Fusion, vol. 62, pp. 32–46, Oct. 2020, doi: 10.1016/j.inffus.2020.03.004.
[33] A. S. Shibghatullah and I. Al Barazanchi, "An Analysis of the Requirements for Efficient Protocols in WBAN," J. Telecommun. Electron. Comput. Eng., vol. 6, no. 2, pp. 19–22, 2014.
[34] S. A. M. Al-Juboori, F. Hazzaa, S. Salih, Z. S. Jabbar, and H. M. Gheni, "Man-in-the-middle and denial of service attacks detection using machine learning algorithms," Bull. Electr. Eng. Informatics, vol. 12, no. 1, pp. 418–426, Feb. 2023, doi: 10.11591/eei.v12i1.4555.