Journal of Theoretical and Applied Information Technology
15th April 2026. Vol.104. No.7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL META-REINFORCEMENT FAST LEARNING NETWORK FOR AN ENERGY EFFICIENT FOG ENABLED IOT ENVIRONMENT

G. PRABHAKAR [1*], MEERAVALI SHAIK[2]

[1]Research Scholar, Department of Computer Science and Engineering, MallaReddy University, Hyderabad, Telangana,500100, India.

[2]Professor, Department of Computer Science and Engineering,MallaReddy University, Hyderabad, Telangana, 500100, India.

Email: prabhakarm.tech@gmail.com (Corresponding Author), meeravali@mallareddyuniversity.ac.in

ABSTRACT

Internet Enabled Devices has opened its wide dimension of applications in the multiple areas such as healthcare, transportation and automation systems. As the computing devices increases, Internet connected devices generates the more number of data which leads to the scarcity of energy and computation. Fog computing has emerged as an innovative paradigm to enhance these devices in terms of energy and time by bringing the computation closer to the data sources. However, a dynamic characteristics of the networks and heterogeneous data in the Internet enabled network poses the serious challenge that affects the network performance to achieve the low latency and energy efficiency simultaneously. To overcome this limitations, this research introduces a novel meta-reinforcement fast learning algorithm for energy-efficient routing and scheduling in the Fog enabled IoT environment. The suggested framework integrates the principle of reinforcement learning and fast neural networks to enable rapid adaptation of routing policies and optimizes the networks by minimizing the transmission latency and energy consumption in the Fog gateways. The framework was deployed in the flexible python based environment (FogBus2 and SimPy) and demonstrated its strong performance by evaluating the quality of services(QoS) metrics such as average latency, energy and resource utilization process. To prove the efficacy of the suggested reinforced technique, its performance was compared with the other techniques. Evaluation results demonstrates that the suggested model balances network characteristics and its performance by achieving the lower transmission latency(54% lesser than traditional methods),consuming only 40% of energy than the conventional learning techniques. The suggested research provides the better insights for scalable and intelligent solutions for an energy efficient Fog computing systems.

Keywords: *Fog Computing, Meta-Reinforcement, Fast Learning Networks,Internet Enabled Devices, Quality Of Services.*

1.INTRODUCTION

Internet of things(IoT) has witnessed the global explosive intrusion in individual's life style by proliferation of various smart devices across consumer and infrastructure domains[1-3]. Nearly 20 billion active Internet connected devices are deployed across the different domains that aids for an effective monitoring, automation and cognitive decision making techniques. It has been estimated that the installed base of connected IoT devices is projected to reach 22 billion, reflecting its growth in terms of adapting it in the organization and consumer ' day to day life[4-7]. Furthermore, pervasive nature of the IoT driven systems provides enhanced intelligence through the continuous sensing and analytics, which finds its applications in the various domains such as smart health care and smart cities[8-10].

Despite its own advantages, Internet of Things(IoT) suffers from the high computational overhead due to the continuous data transmission and frequent sensing[11-13]. As the number of devices increases exponentially to the number of users, this excessive data transmission leads to the traffic congestion, increased packet collision and high latency transmission[14]. In the traditional cloud based IoT architectures, raw user data is often transmitted directly to remote cloud servers for processing, resulting in increased bandwidth consumption and inefficient utilization of network resources.

To overcome this limitations, Fog gateways are introduced in the IoT ecosystems for a computational less data transmission process. The Open Fog Consortium defines Fog Computing as a promising computing framework to resolve the inherent issues of existing cloud computing models regarding bandwidth, delay and storage[15-17]. These Fog gateways are deployed nearer to the IoT source devices rather than forwarding the user data to the cloud for the further processing. Despite its significant advantages, Fog computing suffers from the several challenges such as computational overhead, storage and energy efficient networking capabilities.

Motivated by aforementioned challenge, this research paper proposes Fog driven Reinforcement Fast neural networks for an adaptive routing algorithm in the Fog environments to reduce the computational overhead, energy and latency in the smart ecosystems. The suggested learning algorithms employs the band-width, link delay, energy-level and queue length as the main input factors and each Fog nodes as the agents for determining the energy-efficient routing decisions in an IoT environment. The suggested model was deployed using the Python based environment and various evaluation metrics are calculated and compared with the other learning models. The key contribution of the research is as follows

1. The novel meta-reinforcement learning technique was introduced in the suggested framework to achieve the less computational overhead and energy-efficient routing path in Fog driven IoT environment.
2. The research introduces the fast neural networks integrated with the RL framework for the better identification of QoS- Aware routing path in the Fog-IoT networks
3. The paper introduces the synthetic benchmark dataset collection using the FogBus2 and SimPy framework for emulating the fog computing environment. The testbed captures the diverse traffic patterns, time-delay , energy consumption an throughputs. The proposed test bench provides the intelligent data set collection which is used for validating the suggested framework.
4. The comprehensive experimentation has been conducted on the synthetic benchmarks and QoS metrics are calculated. Experimental results are compared with the other traditional model in which the suggested integration has achieved the more energy efficient and less computational overhead.

The rest of the paper is organized as follows :: **Section-2** describes the related works of existing works and their challenges are also elaborated. The detail of the system model has been provided **in Section-3**.**Section- 4** presents the result outcomes and comparative analysis. Finally, the article concludes with a summary of work and future scope in **Section -5.**

2.RELATED WORKS

Chaudhari et al. (2025) [18] have developed a framework for IoT-enabled smart cities that uses FHE-based MAES and DHGNN for secure data transmission and attack detection. This allows the framework to protect data confidentiality during data transmission and to detect cyberattacks simultaneously in IoT-enabled networks. By utilizing FHE, it will enable computations on encrypted data, thereby enhancing privacy preservation. With this, the DHGNN model focuses on capturing complex relationships in IoT networks for accurate attack detection. Experimental results were presented which showed a superior security approach against attacks with lower severity and promising transmission performance. Its major benefit stems from the integration between encryption and intelligent detection. Its drawback is additional latency overhead introduced by FHE computations. Scalability to large-scale IoT deployments is challenging.

Mehri et al. (2025) [19] have given a clear analysis on the applications of machine learning for optimal data transfer in the context of the Internet of Things. The paper has discussed the applications of several machine learning algorithms for routing, congestion, and data preprocessing. The analysis included improvements in data transfer, packet loss, and adaptability. A significant aspect of this analysis is that it makes a comparison of algorithms for applications in the Internet of Things. The paper discusses drawbacks like resource and real-time learning. The drawback, however, is that it lacks practical testing for performance analysis using

the Internet of Things. Its analysis for security purposes doesn't add much value.

Osman et al. (2024) [20] developed an optimized IoT communication system for smarter farming ecosystems for improving the efficiency of data communication. The system utilizes intelligent optimization methods for improving bandwidth and communication delay. The experimental outcome proves the effectiveness of reliable data communication and energy consumption. This system efficiently supports real-time monitoring in agriculture. The significant benefit of this method is that it optimizes specific applications related to smarter farming. Unfortunately, the security issues related to data communication were not taken into proper consideration. The system considers a stable network environment.

Chinthamu et al. (2023) [21] proposed an IoT secure data transmission prediction model using deep learning in a cloud computing environment. The proposed model predicts data transmission and possible failure occurrences for improved data reliability. Results obtained from experimentation revealed an improvement in accuracy and a reduction in data losses. Deep learning helped in effectively dealing with a huge amount of data from IoT networks. One of its key benefits is the predictive control of data transmission. The cloud dependency can cause delay and cloud failure points. Scaling was not taken into consideration with large-scale IoT networks. There was a lack of security aspects related to prediction approaches.

Stergiou et al. (2023) [22] introduced a secured and robust framework for the transmission and management process for big data using the Internet of Things in a digital twin in the healthcare domain. The proposed framework uses the Internet of Things, cloud computing, and digital twin concepts. The proposed approach ensures secured and efficient data processing. The experimental outcomes showed enhanced integrity, data transmission, and interoperability. The proposed approach provides real-time data for healthcare applications. The prominent aspect includes domain-specific secured integration. The complexity and resource requirement are high. Moreover, scalability in various healthcare settings is very difficult.

Barron et al. (2022) [23] focused on efficient delivery and storage solutions of IoT data in edge-fog-cloud paradigms. Research work with efficient design aims at minimizing latency and storage costs. Results obtained highlighted low latency and effective resource management. The work is beneficial as it increases robustness. One of its strengths is effective workload allocation to layers of computation. The work lacks proper emphasis on security features. The model takes care of trust in nodes at the edge and fog layers. The issue of dealing with malicious nodes is addressed in the work.

Farhan et al. (2021) [24] developed a reliable data transmission and remote monitoring system for IoT use cases. The system provides a combination of optimized communication protocols that guarantee error-free data transfer. The system was evaluated using experimentation, and the results proved a decrease in transmission delay and increased monitoring precision. The methodological technique is appropriate for healthcare and manufacturing IoT systems. The system boasts a low complexity level and easy implementation. The methodological technique has a negligible impact on security and privacy issues. There were no sophisticated attack detection systems. Also, the system's scalability for handling high data traffic was not examined.

Izaddoost et al. (2020) [25] A framework for efficient data transmission with minimal energy consumption for IoT platforms. The method is aimed at optimizing energy consumption in communication. The simulation outcome proved that it is an efficient technique that saves considerable amounts of energy and extends the lifetime of devices. It can be used in IoT networks that are powered by batteries. One great advantage is that it increases the sustainability of IoT networks. It does not make use of intelligent attack detection.

Table 1 Summary of Related works

Author & Year	Focus Area	Proposed Method	Key Contribution	Limitation
Chaudhari et al. (2025)	Smart city IoT security	FHE-based MAES with DHGNN	Secure data transmission and attack detection	High latency and scalability issues
Mehri et al. (2025)	IoT data transfer	ML-based analytical study	Improved data transfer and	No real-time IoT validation;

Author & Year	Focus Area	Proposed Method	Key Contribution	Limitation
			adaptability	limited security
Osman et al. (2024)	Smart farming IoT	Optimization-based communication	Reduced delay and energy consumption	Security not considered
Chinthamu et al. (2023)	Cloud-based IoT prediction	Deep learning model	Improved reliability and reduced data loss	Cloud dependency and limited scalability
Stergiou et al. (2023)	Healthcare digital twin	IoT–cloud–DT integration	Secure and real-time healthcare data	High complexity and poor scalability
Barron et al. (2022)	Edge–fog–cloud IoT	Layered workload allocation	Low latency and efficient resource use	Limited security focus
Farhan et al. (2021)	IoT monitoring systems	Optimized communication protocols	Reduced delay and easy deployment	Weak security and untested scalability
Izaddoost et al. (2020)	Energy-efficient IoT	Energy-aware transmission	Extended device lifetime	No attack detection

3.SUGGESTED SYSTEMATIC FRAMEWORK

As demonstrated in Figure 1, FogBase2 and SimPy is utilized to generate the synthetic test benches which comprises of Fog nodes and gateways. Nearly 50 nodes are simulated in which the health care applications are provided by the Fog nodes. The fog computing layers consist of a finite number of heterogeneous fog computing devices to access the data from the IoT and transmits to the cloud for the further processing. Each Fog services are characterised by the input data and various traffic attributes are collected and used for training the suggested model. Followed by the data collection and gathering process, data pre-processing technique is adopted for cleaning the data. Finally the model are designed ad evaluated using the collected datasets in which QoS aware routing path has been determined.

3.1 System Model

The system model considered for proposed Fog topology which are simulated in Fog2B**.** The model consist of multiple IoT devices connected to a multiple Fog gateway. Each device can communicate with the other devices only through the gateways. Each Fog nodes are integrated with the node_IDsThe system model assumes the proposed protocol network topology is set up in a secure area where attackers have no physical access to the devices. Thus, they cannot discover the configured secret keys that are stored on the devices. Furthermore, MQTT protocol is used for data communication between the Fog gateways, IoT devices and Cloud .

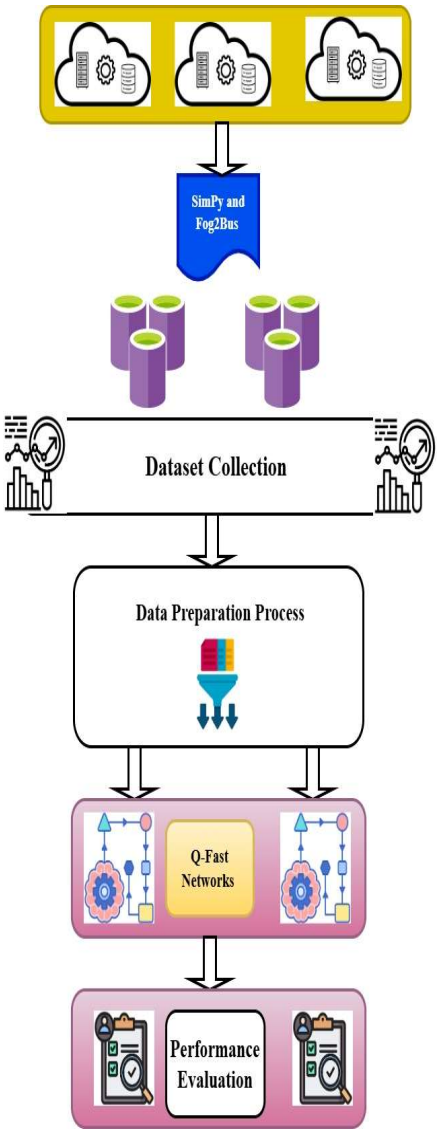

Figure 1 Complete Flow Architecture for the Suggested Routing Framework

3.2 FOG BASED DATASETS TEST-BENCH

In this research, a Python- based Fog Simulation environment is developed by integrating the two different frameworks such as FogBus2 and SimPy[26]. SimPy is a discrete event simulation framework which encompasses the realistic modelling of Fog-enabled IoT systems while maintaining low experimental with the established fog networks. FogBus2 is a lightweight fog and edge computing framework designed to enable the dynamic task scheduling , heterogeneous fog nodes and cloud resources. It adopts a gateway-centric FIFOmodel, where the requests from the IoT nodes are first received by a fog gateway and subsequently allocated to appropriate fog nodes based on quality-of-service (QoS) requirements and resource availability. For an efficient simulation environment, 50 Fog nodes are simulated in which the detailed logs are recorded for each incoming tasks that includes the node identifier, fog nodes, arrival time, start time ,estimated time, latency and energy consumption(E_c). These recorded logs are stored in separate databases which can be used for the complete validation and training the suggested model. Additionally, task arrival rates, network size are also extracted for offering the level of flexibility in the obtained datasets. Table2 presents the data samples collected from the simulation environment

Table 2 Simulation Datasets Collected for the Training the Fog Models

N_ ID	Fog_ Nodes	Arrival _Time	Estimated_Time	Latency	E_c
1	1	0.63732	0.56333	0.4232	0.01425
2	2	0.456622	0.34222	0.23190	0.01902
3	3	0.3242	0.5622	0.6222	0.0182
4	4	0.67222	0.54353	0.3421	0.0383
5	5	0.53422	0.6432	0.4443	0.02425
6	6	0.7332	0.3422	0.2892	0.00222
7	7	0.6532	0.6373	0.443	0.0022
8	8	0.6332	0.5362	0.422	0.0032
9	9	0.5633	0.3242	0.372	0.0422
10	10	0.32422	0.3242	0.672	0.0289

Figure 2 presents the energy fluctuations across the different tasks collected in the simulated environment. The observed fluctuations in energy consumption across the nodes are primarily due to the variations in thecomputational requirements or those assigned to fog nodes with higher energy rates result in increased energy consumption, whereas less taks processed by energy-efficient nodes consume less energy. Figure 3 demonstrates the clear positive correlation between application response time and energy consumption. Tasks with lower response times generally consume less energy, indicating efficient execution on lightly loaded fog nodes. In contrast, tasks experiencing higher

response times tend to incur increased energy consumption, which can be attributed to longer execution durations, queueing delays, or assignment to energy-intensive fog nodes. This behaviour reflects realistic fog computing conditions, where performance optimization often comes at the cost of increased energy usage.

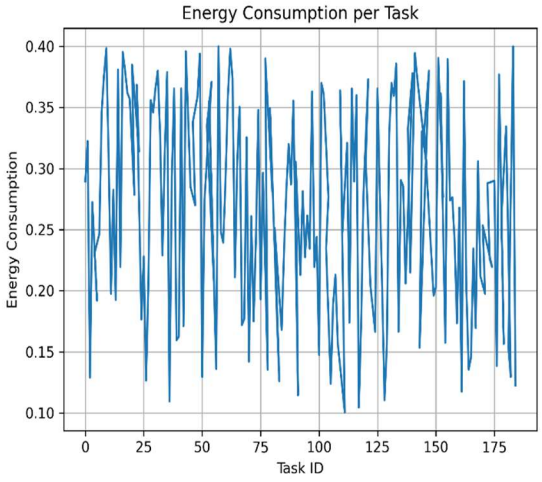

Figure 2 Energy Consumption Datasets per Simulation Task in Integrated Environment

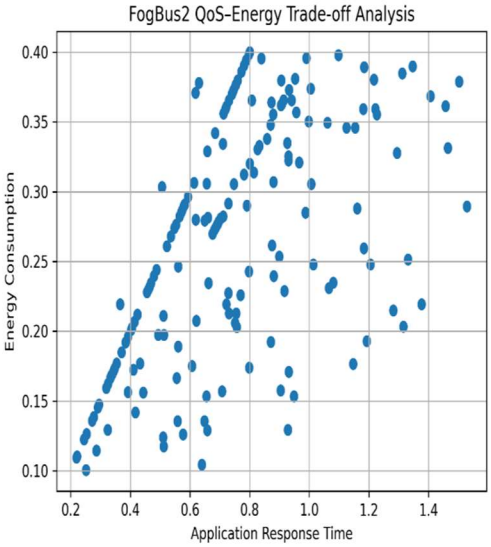

Figure 3 Energy Consumption Datasets per Response time in Integrated Environment

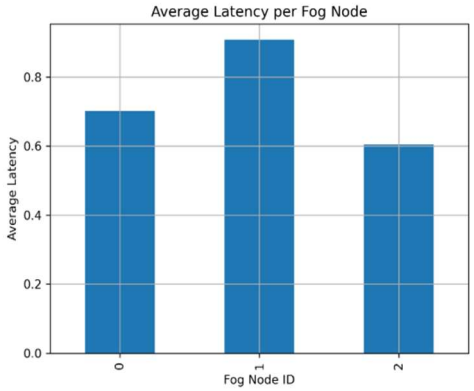

Figure 4 Average Latency for 3 Fog Nodes in Integrated Environment

Figure 4 presents the average latency for three nodes in the integrated environment which clearly states that the latency consumed based on the energy consumption and computational overhead of each fog nodes in the networks. Nearly 18000 data points are collected in which the 70% of data are used for training and 30% are used as testing process.

3.3 DATA PRE-PROCESSING

Data pre-processing is regarded as a key procedure for ensuring the effectiveness of a learning model. It involves tasks such as data cleaning, conversion, and normalization. Initially, all missing and NaN values are excluded from the dataset.Following the removal of missing values , cloud affected areas are filtered by adopting the quality masks and noises are overcome by adopting the smoothening and interpolation techniquesFinally, feature normalization is performed on the datasets, converting all input attributes into a uniform scale. This process is vital to prevent inconsistencies and biases during model learning. In this study, the Min–Max normalization technique is employed, which linearly rescales each feature to a fixed interval between 0 and 1, ensuring uniformity across the collected data.

3.4 RL-FN MODEL DESIGN

The section discusses about the fast neural networks, and hybrid Q-evoked model for the better detection of optimized routing path in the Fog –IoT networks

3.4.1 Fast Neural Networks

The research incorporates the fast neural networks which is constructed following the concept of Extreme Learning Machines. The random assignment of the weights and minimum training error tends to regularize the performance of the model yielding the good performances.

In this type of the system, the 'N' neurons in the hidden layers utilize a continuously differentiable activation operation in which the sigmoid activation functions are used in the intermediate layers and linear activation operation in the output layers. Especially, the initial weight parameters and bias values of the hidden values are randomly assigned in which the bias terms and remains fixed throughput the training process. This characteristic significantly reduces training complexity while maintaining effective learning performance. The output function from the ELM networks are illustrated as follows

$$O(x) = \sum_{i=1}^{LN} \alpha_i G_i(x) = G(x)\alpha \quad (1)$$

$G(x)$→output hidden layers

The working mechanism of Fast Neworks can be expressed mathematically and implements the minimal nonlinear least-square approach, which are represented in equation (2)

$$\alpha' = G^{*}Y = G^{T}(GG^{T})^{-1}Y \quad (2)$$

Where H∗ represent as inverse of H known as Moore–Penrose generalized inverse.

Above equation can also be given as follows

$$\alpha' = G^{T}(\frac{1}{C}GG^{T})^{-1}Y \quad (3)$$

Therefore, the output function can be obtained by using the above equation

$$O(x) = G(x)\alpha = G(x)G^{T}(\frac{1}{C}GG^{T})^{-1}Y \quad (4)$$

Where G(x) denotes maps the input feature , α represents as temporal matrix and C is constant, Finally, the probability of occurrence of each attacks are is calculated by the activation function(softmax), as shown in

$$T' = Softmax(O(x)) \quad (5)$$

Y' is the output to predict multiple attacks in the VANET, cross-entropy function is utilized for the calculation of loss function with the mathematical expression is given as

$$Loss = (\frac{1}{K})\sum_{i=1}^{K}(Y(i) * Log\ Y' + \eta||\theta||^{2} \quad (6)$$

Where K is the dimensional capsule feature length,η *is the* regularization co-efficient and $|\theta|$ is the constant.

3.4.2 RL-FN Model Design

This section details about the Q-based reinforcement learning techniques integrated with the fast learning networks. The research incorporates the model free reinforcement learning that enables intelligent agents to learn the optimal decision through the interaction with a dynamic environment. The major advantage of the integrating the Q-learning in the Fog environment is to learn adaptive routing policies based on real-time applications. The integrating the fast learning networks in the Q-Learning environment. In the suggested Q-Learning model, fast learning networks act as a approximate factor for the different policies values enabling high speed computation process suitable for the fog nodes , which operates with the limited resources and energy consumption. In the suggested fog environments, each simulated fog gateways acts as a learning agent that observes current network state such as fog nodes, arrival time, start time ,estimated time, latency and energy consumption(E_c) and selects the routing action.The reward function is designed to optimize multiple objectives, including minimizing application response time(latency), reducing energy consumption, and improving load balancing across fog nodes. By continuously updating the output weightsof the networks based on reinforcement feedback, the routing policy adapts to changing network conditions and workload patterns. As a result, suggested training model achieves faster convergence, better generalization, and improved quality of service compared to static routing and deep reinforcement learning–based solutions, making it an effective and scalable approach for intelligent routing in fog computing networks.

The model uses the Markov Decision Process for an effective strategy which is used to trigger the parameters for states action, reward and probability of occurences.Let $z$is current

state and z' is the next state with action value a.

$$P_{zz'}^{a} = Prob\{z_{i+1} = z' | z_t = z, a_t = a\} \quad (7)$$

Steps	Working Mechanism for Suggested Framework
1	Inputs : Arrival time , Fog Nodes, Energy Consumption ,Latency
2	Outputs : Best Routing path
3	While(True)
4	Randomly Initialize the Weights of the Fast Neural Networks
5	For each round
6	Obtain the current network status of the Fog environment
7	Calculate the Q-levels from the each fog nodes in the networks
8	Observe the reward function and moves to the next state of the Fog nodes
9	Forward the values to the next fog nodes and accepting the values
10	Output function is calculated using Equation
11	Update the Q-values, Outputs and reward function
12	End For
13	End While

The reward function for state z and z' is given as $R_{z_t z_{t+1}}^{a}.t$.The overall reward function of current state is

$$R_t = \alpha D(t) + \beta E(t) + \mu A(t) \quad (8)$$

where D(t) is the total time required for transmission.

$E(t)$ *is the Energy consumption*

A(t) is the arrival time /response time. The output ELM functions are updated using the Q-learning policies which is illustratedby modifying the $O(x) = G(x)QT = G(x)G^T(\frac{1}{C}GG^T)^{-1}QT(9)$

Equation(9).

The complete working of the suggested RL-FNN based routing mechanism is illustrated in Algorithm-1

4. EXPERIMENTAL OUTCOMES

The envisioned framework has been implemented using Python3.19 and Fog2Bases2 with Simpy environment.To prove the superiority of the proposed model, existing machine learning algorithms(without reinforcement) has been considered for the experimentation ande demonstration process. The metrics such as packet delivery ratio(PDR), control packet overhead(CPO) and throughput are evaluated and compared with the other existing models. This evaluation was carried out by varying the number of iterations that ranges from 200 to 1500 iterations respectively.Intel core i7 processor 3.55GHz processor and 16 GB RAM The simulation parameters for the proposed algorithms are provided in Table 3.

Table 3 Simulation Parameters for the Experimentation

Specifications	Simulation parameters
Number of Cloud Layered Devices	10
Number of Fog Devices	50
Number of End Devices	50
Applications Installed in Networks	01
Number of Tasks Transmitted	50
Number of Service Space Requirements	10
Initial Energy at Fog Nodes	0.1J

4.2 Performance Outcome Analysis

As mentioned in previous section, this section demonstrates the performance metrics of the different models in identifying the QoS related paths in Fog nodes

4.2.1 End-to-End Delay Analysis

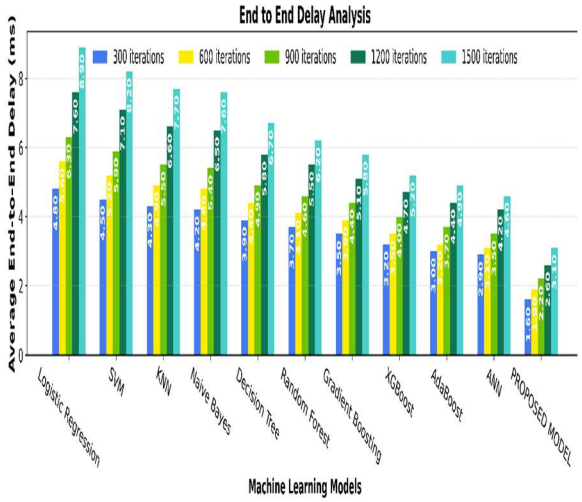

Figure 5. End-to-End Delay Analysis of Routing Protocols in FOG–IoT Environment

Minimizing end-to-end delay is an ever-existing challenge in FOG-IoT routing networks, particularly for real-time and delay-sensitive applications. To tackle this situation effectively, we require efficient routing techniques capable of transferring data from source to destination with a fast and trusted procedure because every millisecond counts in real-time decision-making and safety-critical systems. From Figure 5, we analyze the end-to-end delay comparison of various machine learning-based FOG-IoT routing models when the number of iterations increases from 300 to 1500 levels. The existing approaches, including LR, SVM, KNN, and NB models, increase end-to-end delays with an increase in the number of iterations since their paths are not optimized effectively in comparison to others. For all levels of iterations, the proposed method demonstrates a consistent minimum end-to-end delay of approximately 1.3 ms in a 1500-level iteration scenario because of its efficient selection of low-delay paths in FOG-IoT routing systems.

4.2.2 Average Packet Delivery Ratio

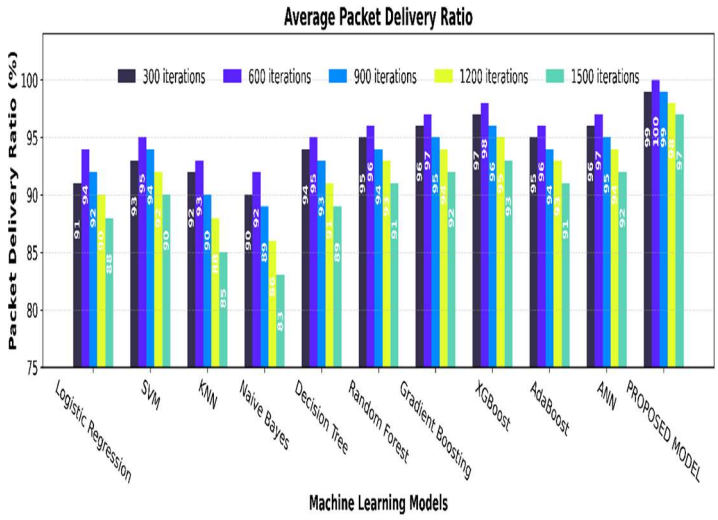

Figure 6. Average Packet Delivery Ratio of Routing Protocols in the FOG–IoT Environment

PDR signifies reliability exists in transmitting data over FOG–IoT networks. Figure 6 shows the average PDR of various machine learning-driven routing models at different iteration levels starting from 300 to 1500 respectively. Traditional models have a poor PDR since they are not capable of adapting well, while ensemble methods offer some improvements. The proposed model always leads the chart with approximately 99% PDR at 1500 iterations and hence establishes its efficiency in reliable and efficient data delivery in FOG–IoT environments.

Journal of Theoretical and Applied Information Technology
15th April 2026. Vol.104. No.7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2.3 Throughput Analysis :

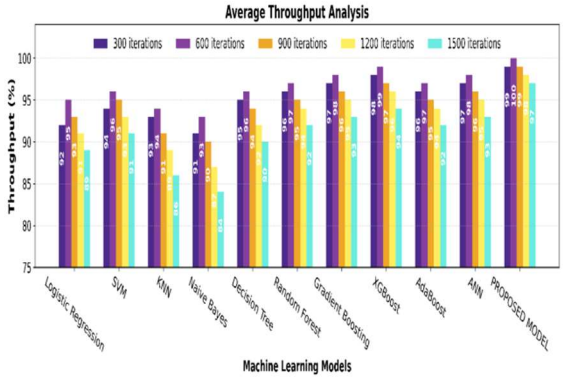

Figure 7. Comparison of Average Throughput for Optimized FOG–IoT Routing Schemes

Throughput demonstrates network data movement efficiency in FOG-IoT communications. The greater the value, the better resource utilization and a critical requirement in data-intensive, real-time IoT operations. From Figure 8, different routing ML model average throughput values are shown based on levels from 300 iterations to 1500 iterations. The conventional model exhibits low values, whereas innovative and learning-driven techniques improve throughput values. The proposed approach always ranks first at 98% with 1500 iterations, reflecting a highly effective routing process in FOG-IoT communications with high demands on data movement.

4.2.4 Residual Energy Analysis :

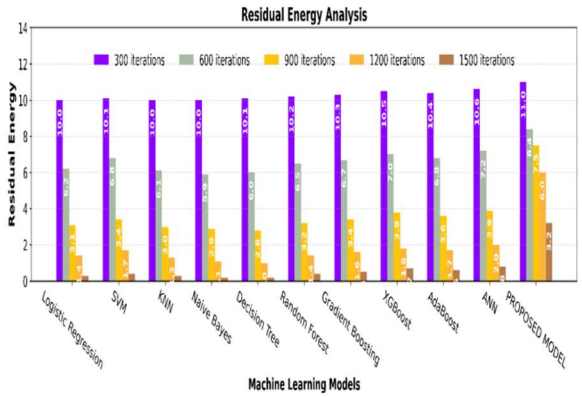

Figure 8. Analysis of Residual Energy for FOG–IoT Routing Protocols

Figure 8 shows how residual energy evolves for various routing models-from Logistic Regression and Naïve Bayes to SVM, KNN, Decision Tree, Random Forest, Gradient Boosting, XGBoost, AdaBoost, ANN, and the model we propose-tracked over 300 to 1500 iterations. The classic methods, Logistic Regression and Naïve Bayes, have a tremendous burn of energy, with residual energy less than 1.0 at 1500. Learning-based schemes like Random Forest, Gradient Boosting, and XGBoost hold their energy better compared to the rest but have a fading characteristic as time progresses. Our proposed model is always able to hold the highest residual energy: roughly 11.0, 8.4, 7.5, 5.6, and 3.2 at 300, 600, 900, 1200, and 1500 iterations, respectively. This is due to the highly efficient path selection together with fewer retransmissions, a characteristic that makes this approach suitable for energy-constrained FOG–IoT environments.

4.2.5 Mean Routing Load Analysis:

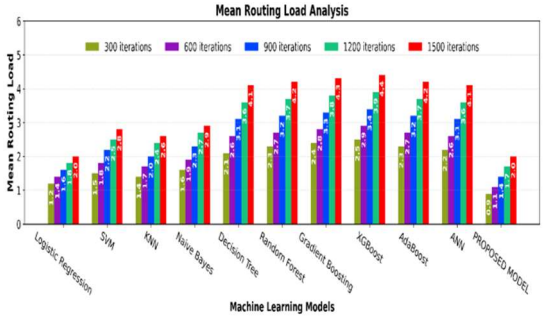

Figure 9. Analysis of Mean Routing Load in FOG–IoT Routing Protocols

Figure 10 presents the average routing load for different ML-based routing models, monitored as iterations run from 300 to up to 1500 respectively. Classic models, such as Logistic Regression, SVM, KNN, and Naïve Bayes, have the tendency to increase the routing load as iterations increase, since these methods trigger more route updates and have a weak control on path management. Tree-based and boosting methods include Decision Tree, Random Forest, Gradient Boosting, XGBoost, and AdaBoost, which also reveal better performance but still incur a fair level of routing overhead. Compared to other models, our proposed model delivers the lowest mean routing load at every iteration level and stays near 1.0 even at 1500 iterations. It gains this merit due to smarter route selection and a reduced number of control packet transmissions. In other words, this approach is well scalable and suitable for resource-limited FOG-IoT routing environments.

4.2.6 Packet Overhead Analysis :

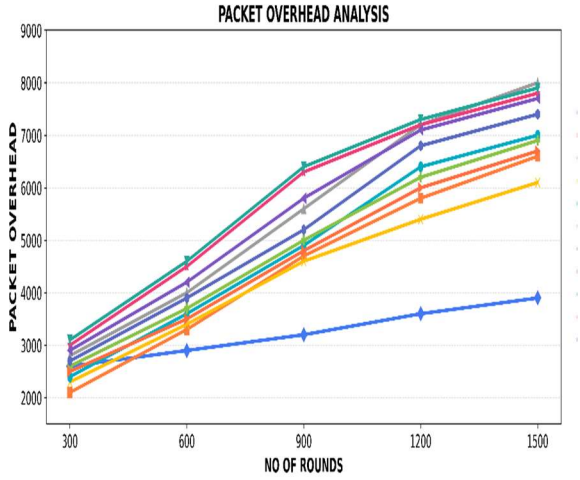

Figure 10. Packet Overhead Performance of Routing Protocols in the FOG–IoT Environment

Figure 10 focuses on the increase in packet overhead with the number of routing rounds varying from 300 to 1500 for different ML-based routing models. Conventional techniques such as Logistic Regression, SVM, KNN, Naive Bayes, Decision Trees, increase steadily in packet overhead. For instance, Logistic Regression rises from 2200 to 6700 packets, whereas KNN rises from 2400 to 6100 packets. Naive Bayes and Decision Trees are in the range of 3000-7800 packets and 2800-8000 packets, respectively, at 1500 routing rounds, thus indicating an increase in control packets as well as routing activities. The advanced learning models perform relatively better but with a considerable overhead as the value of rounds increases. The Random Forest increases from 2700 to 7400 packets, Gradient Boost from 2900 to 7800 packets, XGBoost from 3100 to 8000, AdaBoost from 2600 to 7000 packets, and ANN from 2900 to 7600 packets. In contrast, in the proposed system, the minimum number of packet overhead is maintained constantly and increases only from about 2600 packets at 300 rounds to 3900 at 1500 rounds. This is because of improved route discoveries and reduced control packets in the proposed strategy, which makes it even more suitable for a scalable and energy-efficient FOG-IoT networking system.

5. CONLCUSION AND FUTURE DIRECTION

This research article introducesnovel RL-FN networks for determining the QoS effective routing paths in Fog enabled IoT environment. The suggested framework effectively integrates the reinforcement learning with the fast neural networks to enable the rapid policy adaptation and reward –enabled QoS aware optimization under dynamic Fog network conditions. The suggested model significantly reduces the latency and energy consumption process, by which increases the performance and efficiency of the networks. The research also introduces the novel data generation test bench which comprises of SimPy and Fog2Base to generate the numerous data patterns under the various traffic conditions. Extensive experimentation has been conducted in which the various QoS metrics are calculated and compared with the other traditional machine learning algorithms. Simulation results demonstrates that the suggested model has shown the enhanced performances than the existing models with the less latency and energy efficient Fog based routing algorithms. As the future direction, Explainable reinforcement learning, enabling transparent decisions in terms of health care and smart automation systems. Finally, the framework should be enable for the real time test beds and large scale deployments, along with the adversarial attacks that challenges the reliability and robustness of the systems.

REFERENCES

[1] Behera, T.M.; Samal, U.C.; Mohapatra, S.K.; Khan, M.S.; Appasani, B.; Bizon, N.; Thounthong, P. Energy-Efficient RoutingProtocols forWireless Sensor Networks: Architectures, Strategies, and Performance. Electronics **2022**, 11, 2282.

[2] Maheshwari, P.; Sharma, A.K.; Verma, K. Energy efficient cluster based routing protocol for WSN using butterfly optimizationalgorithm and ant colony optimization. Ad. Hoc. Netw. **2021**, 110, 102317.

[3] Xu, C.; Xiong, Z.; Zhao, G.; Yu, S. An energy-efficient region source routing protocol for lifetime maximization in WSN. IEEEAccess **2019**, 7, 135277–135289.

[4] Alencar, R. C., Fernandes, B. J. T., Lima, P. H. E. S., & da Silva, C. M. R. (2024). AI techniques for automated penetration testing in MQTT networks: a literature investigation. *International Journal of Computers and Applications*, *47*(1), 106–121. https://doi.org/10.1080/1206212X.2024.2443504

[5] Hmissi, F., &Ouni, S. (2022). TD-MQTT: Transparent Distributed MQTT Brokers for Horizontal IoT Applications. *2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 479-486.

[6] Bangare, P. S., &Patil, K. P. (2024). Enhancing MQTT security for internet of things: Lightweight two-way authorization and authentication with advanced security measures. *Measurement: Sensors, 33*, 101212. https://doi.org/10.1016/j.measen.2024.101212

[7] M. Ali Al-Muqarm, Abbas &Alkhafajee, Ahmed &Alwan, Ali &Alardawy, Zaid. (2022). Security and Performance Analysis of MQTT Protocol with TLS in IoT Networks. 10.1109/IICETA51758.2021.9717495.

[8] F. A. Shodiq, R. R. Pahlevi and P. Sukarno, "Secure MQTT Authentication and Message Exchange Methods for IoT Constrained Device," *2021 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)*, Bandung, Indonesia, 2021, pp. 70-74, doi: 10.1109/ICICyTA53712.2021.9689126.

[9] Liu, Z., Liang, T., Lyu, J., & Lang, D. (2024). A security-enhanced scheme for MQTT protocol based on domestic cryptographic algorithm. *Computer Communications, 221*, 1–9. https://doi.org/10.1016/j.comcom.2024.04.013

[10] Sundarrajan, M., Narayanan, A. E., &Srithar, V. (2021). Securing the MQTT protocol using enhanced cryptographic techniques in IoT surroundings. *Journal of Physics: Conference Series, 1767*(1), 012055. https://doi.org/10.1088/1742-6596/1767/1/012055

[11] S. P. Mathews and R. R. Gondkar, "Protocol Recommendation for Message Encryption in MQTT," *2019 International Conference on Data Science and Communication (IconDSC)*, Bangalore, India, 2019, pp. 1-5, doi: 10.1109/IconDSC.2019.8817043.

[12] Hameed, F. M. H., &Kurnaz, S. (2024). An Effective Mechanism for FOG Computing Assisted Function Based on Trustworthy Forwarding Scheme (IOT). *Electronics*, *13*(14), 2715. https://doi.org/10.3390/electronics13142715

[13] Alotaibi, N. S., Sayed Ahmed, H. I., Kamel, S. O. M., &ElKabbany, G. F. (2024). Secure Enhancement for MQTT Protocol Using Distributed Machine Learning Framework. *Sensors*, *24*(5), 1638. https://doi.org/10.3390/s24051638

[14] Hong, S., Park, S., Youn, H., Lee, J., & Kwon, S. (2024). Implementation of Smart Farm Systems Based on Fog Computing in Artificial Intelligence of Things Environments. *Sensors (Basel, Switzerland), 24*.

[15] N. Kadhim, Ola &Ketab, Ahmed &Obaid, Ahmed &Albermany, Salah & Raheem, Ahmed &Hussien, Naseer. (2023). Simulation Secure MQTT Protocol Based on TLS in IoT-Fog Computing Environment. 10.1007/978-981-99-3716-5_2.

[16] Nguyen, H. P., & Chen, Y. (2024). Lightweight, Post-Quantum Secure Cryptography Based on Ascon: Hardware Implementation in Automotive Applications. *Electronics*, *13*(22), 4550. https://doi.org/10.3390/electronics13224550

[17] Roussel, N., Potin, O., Di Pendina, G., Dutertre, J.-M., &Rigaud, J.-B. (2024). Enhancing Security and Power Efficiency of Ascon Hardware Implementation with STT-MRAM. *Electronics*, *13*(17), 3519. https://doi.org/10.3390/electronics13173519

[18] Anita Chaudhari and Rajesh Bansode. (2025). *Secure data transmission and attack detection framework for IoT-enabled smart cities using FHE-Based-MAES and DHGNN.* Expert Systems with Applications. DOI: https://doi.org/10.1016/j.eswa.2025.129314

[19] Ali Mehri. (2025). *Efficient data transmission in IoT systems based on machine learning methods: A short analysis of algorithms, applications, and challenges.* March 2025.

[20] Radwa Ahmed Osman. (2024). *Optimizing IoT communication for enhanced data transmission in smart farming ecosystems.* Expert Systems with Applications. DOI: https://doi.org/10.1016/j.eswa.2024.125879

[21] NarenderChinthamu, Satheesh Kumar Gooda, ChandrasekarVenkatachalam, and Swaminathan S. (2023). *IoT-based secure data transmission prediction using deep learning model in cloud computing.* International Journal of Recent Innovations in Trends in Computing and Communication. DOI: 10.17762/ijritcc.v11i4s.6308.

[22] Christos L. Stergiou, Maria P. Koidou, and Konstantinos E. Psannis. (2023). *IoT-based big data secure transmission and management over cloud system: A healthcare digital twin scenario.* Applied Sciences, 13(16), 9165. DOI: https://doi.org/10.3390/app13169165.

[23] Alfredo Barron, Dante D. Sanchez-Gallegos, Diana Carrizales-Espinoza, J. L. Gonzalez-Compean, and Miguel Morales-Sandoval. (2022). *On the efficient delivery and storage of IoT data in edge–fog–cloud environments.* Sensors, 22(18), 7016. DOI: https://doi.org/10.3390/s22187016.

[24] LaithFarhan, FirasMaanAbdulsattar, LaithAlzubaidi, Mohammed A. Fadhel, BanuÇalışUslu, and Muthana Al-Amidie. (2021). *Efficient data transmission and remote monitoring system for IoT applications.* In Intelligent Data Analytics for Industry 4.0. DOI: https://doi.org/10.1002/9781119792253.ch10.

[25] AlirezaIzaddoost and Matthew Siewierski. (2020). *Energy efficient data transmission in IoTplatforms.*Procedia Computer Science. DOI: 10.1016/j.procs.2020.07.055.

[26] D. Zinoviev, "Discrete Event Simulation: It's Easy with SimPy!," *arXiv preprint arXiv:2405.01562*, Apr. 2024. doi: 10.48550/arXiv.2405.01562.