Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
DOI : 10.47974/JIOS-2116

A lightweight Fog Assisted Cloud Model (FACM) for secure environment

Karthiga Sivakumar [†]
Department of Data Science
Faculty of Science and Humanities
SRM Institute of Science and Technology
Ramapuram Campus
Chennai 600089
Tamil Nadu
India

Sutha Kaliappan *
Department of Computer Science
Faculty of Science and Humanities
SRM Institute of Science and Technology
Ramapuram Campus
Chennai 600089
Tamil Nadu
India

Renuga Devi Ramasamy [§]
Department of Data Science
Faculty of Science and Humanities
SRM Institute of Science and Technology
Ramapuram Campus
Chennai 600089
Tamil Nadu
India

Abstract

Distributed computing is one among the really astonishing innovation in the cutting-edge period because of its productivity in cost-cutting with its adaptability of lessening the own assets while it builds the computational productivity. Continuous protection is

[†] *E-mail:* **karthiga2191@gmail.com**
* *E-mail:* **ksutha1986@gmail.com (Corresponding Author)**
[§] *E-mail:* **drrrenugadevi86@gmail.com**

© Taru Publications

required for today's versatile cloud environments. The massive accessibility of cloud also creates random act of vulnerability. Keeping these constraints as an important consideration, the presented system arrives the solution by developing lightweight cloud environment with Fog-assistance. Fog-assisted cloud computing provides a more distributed, secure, and efficient infrastructure for processing data and delivering services, addressing some of the security challenges associated with traditional cloud-centric approaches. The proposed approach considers the real time data collection through edge sensor networks (ESN). the scenario of data loss during the malfunctioning activities, on the other hand Fog-assisted cloud model (FACM) that tackle the security constraints and retrieve the real parameters is simulated here. The network optimization on malicious activity is adjusted with wind driven optimization (WDO) model. The comparative analysis of both the environment is practically explored with relevant state of art systems.

Subject Classification: *68M14, 68T30.*

Keywords: *Fog computing, Cloud computing, Distributed systems, Secure computing, Cyber security.*

1. Introduction

The emerging growth of internet of things (IoT) enabled systems, the accessibility to the cloud environment for data sharing, storage, processing is increased. Mobile based devices, edge-based devices are keep on communicating with the cloud server for accessing various data. Efficient scheduling of relevant applications to the demanded task is a challenging problem in cloud environment due to mobility factors in IoT networks, resource heterogeneity, uncertainty in behaviour etc. Utilization of recurrent neural networks in the cloud environment improves the performance [1]. Managing the cloud infrastructure is a crucial task. Despite of increasing resource accessibility, the development is still in a

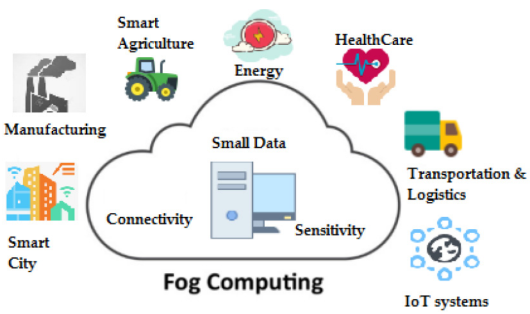

Figure 1

Fog computing architecture

limited condition. Fig 1. shows the fog computing environment capable of communicating with various resources and task scheduler like Manufacturing and mining, Consumer utilization of core IoT, Smart city interfacing, transportation and logistics services, E-Health care analysis, energy and agriculture. The complete shielding over the base connectivity devices such as sensors, cloud server, access control network is created with Fog cloud [2].

Fog computing is employed in smart agriculture management systems, drip irrigation systems, and energy saving in smart irrigation models. The system protocols are applied in transportation and logistics. The manufacturing industry with large data transfers rely on cloud computing mechanism. The foggy clouds enable the data security during loss of battery backup. Highlighted some key applications and benefits of both fog computing and cloud computing. Let's break down the points you mentioned:

Fog Computing in Smart Agriculture:

Fog computing is utilized in smart agriculture management systems to enhance efficiency and decision-making. It brings computing resources closer to the data source (such as sensors in the field), reducing latency and enabling real-time analysis. This is crucial for optimizing irrigation schedules, crop monitoring, and other precision agriculture tasks.

Fog Computing in Drip Irrigation Systems:

Fog computing can improve drip irrigation systems by providing local data processing capabilities. This enables timely analysis of soil moisture, weather conditions, and crop health, leading to more efficient water usage and better crop yields.

Energy Saving in Smart Irrigation Models:

Smart irrigation models leverage fog computing to process sensor data locally and make intelligent decisions about irrigation. By reducing the need for constant data transmission to a distant cloud server, energy consumption is lowered.

Transportation and Logistics Protocols:

Fog computing protocols find application in transportation and logistics. They can be used to optimize routes, manage traffic, monitor vehicle health, and provide real-time updates to drivers. These tasks benefit from lower latency and localized data processing.

Cloud Computing in Manufacturing:

The manufacturing industry often relies on cloud computing for large-scale data storage, analysis, and management. Cloud solutions can handle vast amounts of data from sensors, equipment, and production processes. This enables manufacturers to make informed decisions based on historical and real-time data.

Foggy Clouds and Data Security:

Fog computing, which involves distributing computing resources closer to the data source, can indeed enhance data security in scenarios where there's a potential for loss of battery backup or network connectivity. By having local processing capabilities, sensitive data can be processed and secured within the fog layer even if the main power source is disrupted.

Both fog computing and cloud computing play important roles in various industries, and their combination can provide a holistic solution to address different aspects of data processing, storage, and analysis. The specific choice between fog and cloud computing depends on factors such as latency requirements, data volume, and the need for real-time decision-making.

All it needed is the self-resilience network with automated configurations and fog architecture for support. IoT networks rely on seamless communications from end to end. Cloud computing systems provides various benefits and offers various challenges also. In terms of privacy and security the concern is more since massive data communication is provides vulnerable activity of their party users. To ensure protection of data is crucial [3].

Various applications are integrated in the cloud utilized by the users. After the usage migrating from cloud environment need physical data to be cleared. This may leave the impression of data into the existing cloud. The integrity of trust in the cloud is an important challenge.Resource allocation and scalability is a major constraint. Over allocation or resource utilization leads to performance issues [4]. Managing the cloud environment needs efficient tools. Operational challenges need more customized tools.

- The proposed system is focused on creating a lightweight architecture with fog assisted cloud.

- The primary goal of the system is to provide low latency and immediate optimization of network during malicious activity.
- The proposed model is evaluated with wind driven optimization (WDO) system with Fog assisted cloud model (FACM) to ensure data security.
- The massive drop of data is educed by the fog nodes (FN), data saving is done at fog clusters (FC).

The rest of the paper is formulated as Section 2. Discussing the literature background, Section 3. explores the system tool selection, Section 4. explores the methodology, Section 5. discussed the obtained results. Further the paper is concluded with future scope.

2. Literature Survey

- *Liu et al. [5]* the author presented a fog computing mechanism through parallel offloading approach. Clustering tasks in heterogeneous network are formulated here. The complexity in task distribution in fog computing on multiple host and multi-tasking nodes are considered here for analysis. These challenges are faced through generalized Nash equilibrium (GNE). discussing the challenges and considerations associated with efficiently managing task distribution and multitasking in a fog computing environment, especially in scenarios involving diverse devices with varying capabilities. This type of analysis is crucial for designing effective algorithms and strategies for task management in such environments.
- *Wu and Ansari [6]* In common fog computed devices are composed of fog nodes, clusters, and access controls. The author presented a system where heuristic algorithm is utilized. Blockchain computed systems need more power consumption and more storage space. The presented system demonstrated that cooperative computing model reduces the time taken for hash blocks.the presented system appears to demonstrate the advantages of employing a cooperative computing model to enhance the efficiency of processing hash blocks, leading to reduced processing times compared to traditional methods. This aligns with the general principle of leveraging parallelism and distributed computing to improve the performance of computationally intensive tasks.

- *Ali et al. [7]* Sensitive environments are developed with volunteer supported Fog Computing. The author presented a system where iFogSim toolkit is utilized for managing the distributed computing environments. 93% energy on computation is saved. Distributed computing mechanism with delay-sensitive challenges are analysed here. Various challenges in existing framework is discussed, the role of fog computing enforce the distributed computed model remove the obstacles.
- *Liu et al. [8]* the author presented a vehicular fog computing system to analysed the malicious activity present in the network. The presented system is computed with multiple outsourcing tasks. Boneh-Lynn-Shacham(BLS) algorithm is utilized for digital signature generation and validation for multiple source accessing networks. The presented system having the challenge in anonymous entry during group signature entry. the described system leverages the BLS algorithm to enable secure digital signature generation and validation for multiple sources accessing a network. This helps ensure the authenticity and integrity of communications and interactions within the network while considering the efficiency required for handling multiple outsourcing tasks.
- *Battula et al. [9]* the author presented an energy efficient resource monitoring framework in fog environments. The conventional models utilized in distributed systems are not suitable for fog computing systems. A fog emulator is developed to examine the synthetic fog data. By addressing these challenges, the presented system can offer improved performance, responsiveness, and reliability, leading to a better user experience and effective utilization of the BLS algorithm for digital signature operations in a distributed network.
- *Liang, Zhang and Leung [10]* the author developed a trust computing mechanism in wireless sensor networks. The devices connected at the fog nodes process the data independently and covers the feedback for social sensor enabled cloud. A reliable trust mechanism is created to improve the computational efficiency, reliability etc.
- *Chiu et al. [11]* the author presented a system on Latency driven fog assisted computing in Radio access networks. discussing the establishment of an optimized network to address the challenge of low latency in a hard optimization problem. Additionally, you mention managing limited accessibility in a heterogeneous network using multiple Fog (FoG) groups. Solving a “hard optimization

problem" means finding a solution that meets all requirements while adhering to limitations.Creating multiple Fog groups means organizing these devices into clusters or groups based on their proximity and capabilities.

- *Dong et al. [12]* *t*he author developed a fog computing model for mobile applications. To improve the quality of experience in smart city architecture, created a fairness model. The convex optimization model is deployed here to handle the energy efficient distributed computing. Deploying a convex optimization model to handle energy-efficient distributed computing indicates the use of mathematical optimization techniques to manage energy consumption in a distributed computing environment.
- *Goudarzi, Palaniswami and Buyya [13]* here a distributed deep reinforcement learning model is created for the application of both Edge computing environment and Fog computing environment. A weighted actor learning architecture is utilized for distributed computing. The major challenge faced in this system is that the model gets failed in tackle the applications placement issues.

From various existing developments made so far, it clears in certain scenario that

- Distributed computing mechanism face the problem of data privacy.
- Anonymous entry in massive network is feasible, hence detection of malicious activity needs to be improved.
- Complexity in architecture scope in cloud increases latency, and increased challenge in data distribution at the edges.

3. System Design

Complex architecture created in the cloud environment increases the weight hence increase the latency of the system. Due to malicious activity during the cloud sleep condition, the access control is moved to risk. Distributed computing model ace data privacy challenges at the edges of the network. Keeping these constraints as crucial consideration, the proposed model developed a Fog edge computing to provide Fog assisted cloud model (FACM). The proposed solution involves the development of a Fog-Assisted Cloud Model (FACM). This model likely leverages fog edge computing to provide a more secure and efficient way of managing data and computing resources. The FACM could enhance access control, data privacy, and overall system performance by combining the benefits of both fog and cloud computing. Integrating fog nodes into a cloud infrastructure enhances data security during offline periods, diverts malicious activity from live nodes at the edges, and facilitates secure communication. This approach contributes to a more secure, resilient, and efficient computing environment. Additionally, it mentions the capability of diverting malicious activity from live nodes at the network edges and enabling secure communication.

The strategy aims to make computing environments safer by combining cloud resources with fog edge computing. This is accomplished by dispersing functions for data processing and storage, thereby minimizing the risk to sensitive data. Also, the engineering can carry out more grounded safety efforts at both the haze and cloud levels to protect against different types of cyberattacks.

The architecture of the approach probably makes the system as a whole more resilient. The system is less susceptible to single points of failure when computing tasks are distributed across cloud and fog resources. Assuming thatone part encounters issues, different parts can keep on working, guaranteeing continuous activities and limiting the personal time. The proposed model is developed using MATLAB software with communication toolbox and signal processing toolbox.

4. Methodology

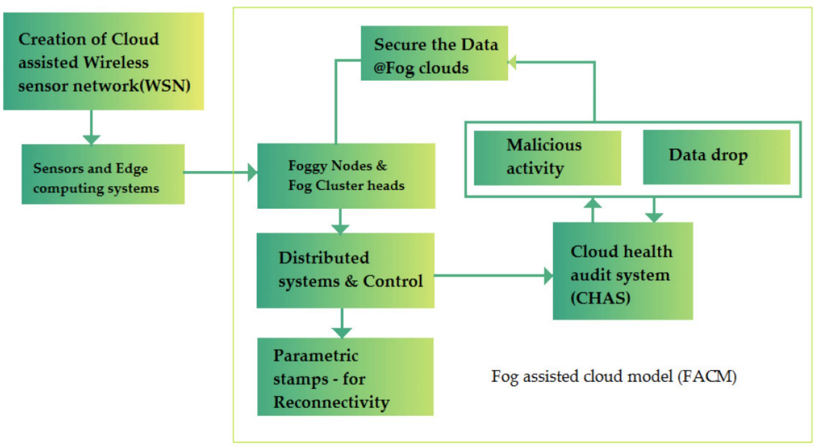

Figure 2

System architecture of proposed FACM

Fig 2. shows the system architecture of proposed FACM for secure data transmission in the cloud. the wireless nodes at the edges are sensors devices, sensor connecting networks and modems. These devices are aligned in a dynamic structure. The sensor nods are kept communicating with each other though the cluster head. The distributed cloud connects with edge devices with mutual authentication.

Fog assisted cloud model (FACM)

The paradigm of FACM is created for the purpose of dual security to the cloud environment offering the health auditing of cloud, monitoring, and securing the data drop rate, malicious activity screening and latency monitor. The novel process aligns the time line work in a finite state activity enabling the complete protection of cloud environment through fog assisted modules.

Sensor nodes relate to fog nodes with fog assisted clusters. These nodes are close to the edge computing devices capable of handling the data source and generation of real time data. These nodes directly communicate with the real time parameters and gather the dynamically changing values.

Fog nodes are formulated into clusters through which the communication establishment is made. Fog nodes on the other hand communicate with the shared nodes and gather information, process it, and collaborate with tasks.

The localized fog nodes filter the data, process it, and analyses the data. The activity is helpful in reducing the latency, improves the bandwidth and summarize the relevant data to cloud.

In fog computing the nodes can collaborate and process the tasks. The distributed network increases the processing quality of data and increases the scalability. Fog computing architecture optimizes the resource usage, reduces the latency to make more efficient data transfer.

Algorithm: FACM_Wind Driven Optimization

```
Output : Optimized Network
Start
Loop 1: For i = 1:Number_of_nodes
Loop 2: For j=1:Number_of_Cluster_Heads
    X=random_probability(data);
Xc=∑Xi,j(cost)
```

If Xe(energy) < threshold, then
Enable Fog_Storage-Authenticate;
If Mal_node(Xi,j) then
Store FogCluster=X;
End
*Apply **WDO**(data X)*
Repeat.
End loop 1
End Loop2

Design procedure

algorithm outline for optimizing a network using a hybrid approach involving FACM (Fog-Assisted Cluster Management) and WDO (Wind Driven Optimization). This algorithm seems to be designed for optimizing network nodes in a fog computing context. Below is a breakdown of the algorithm steps you've provided:

Algorithm Initialization:

Start the algorithm.
Main Loop 1: For Each Node in the Network:
Iterate over each node (i) in the network.
Main Loop 2: For Each Cluster Head:
Iterate over each cluster head (j) in the network.

Generate Random Probability:

Generate a random probability value X.
Calculate Xc:
Calculate the sum of Xi,j for the given cost.

Check Energy Threshold:

If the energy (Xe) is less than a specified threshold:
Enable Fog Storage Authentication.

Check for Malicious Node:

If the current node (Xi,j) is identified as a malicious node:
Store the current Fog Cluster (FogCluster=X).
Apply Wind Driven Optimization (WDO):
Apply the Wind Driven Optimization using data X.

Repeat Main Loop 2:

Repeat the steps in Main Loop 2 for all cluster heads.
Repeat Main Loop 1:
Repeat the steps in Main Loop 1 for all nodes.
End Algorithm:

This algorithm appears to be a fusion of FACM (Fog-Assisted Cluster Management) and WDO (Wind Driven Optimization) to optimize network nodes while considering energy thresholds, malicious node detection, and applying the WDO technique for further optimization

Implementation Summary

- The distributed cloud composed of sensor network each assigned with random cost value and random priority, distance etc.
- These nodes are established into communication through random probability function. The random nodes are controlled by a cluster head.
- The proposed FACM model controlled with WDO process improves the quality of network creation with specified detailing of process variations.
- The FACM model is focused on removing the malicious activity patterns through wind driven optimization and manipulate the network flow in case of low energy.
- The FACM protects the data getting dropped from the cloud systems during consistent drop of energy.
- The system also performs cloud health audit through continuous monitoring and upgradation of distributed system health status.
- Privacy is considered as important factor in optimizing the network as well as the data security in the complete cloud.

5. Results and Discussions

Fig 3. Shows the creation of Fog computing nodes, created through random probability generation through sorting algorithm.The nodes are configured through random distance and random cost. At every cluster head few nodes are randomly connected.

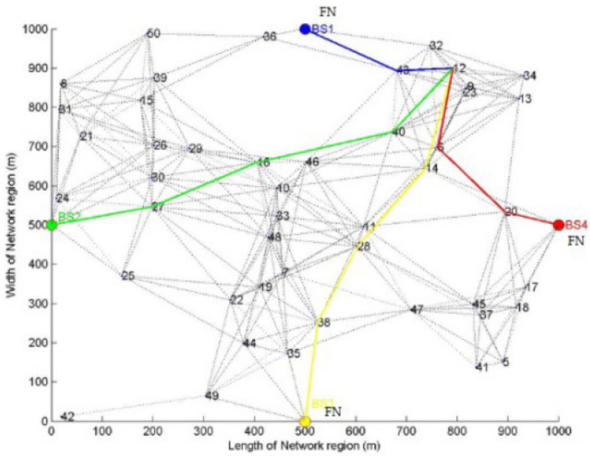

Figure 3

Creation of Fog computed network nodes

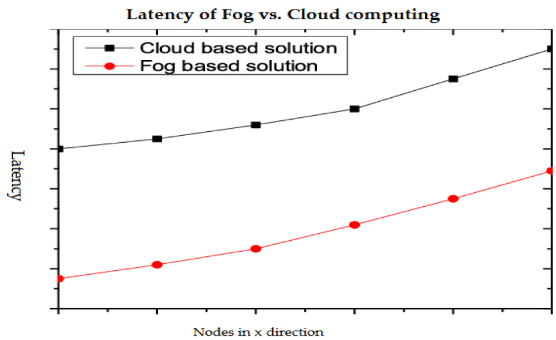

Figure 4

Latency of Fog computing vs. Cloud computing model

Fig 4. shows the latency result of Fog computing vs. Cloud computing systems. For the given nodes in x-direction with respect to relevant latency during communication is shown here. The foggy nodes perform with reduced latency comparing with the cloud computing models.

Fig 5 shows the processing delay of CCM vs.FACM model. Where the delay in complete network processing reduced in FACM with respect to the dynamically varying loops.

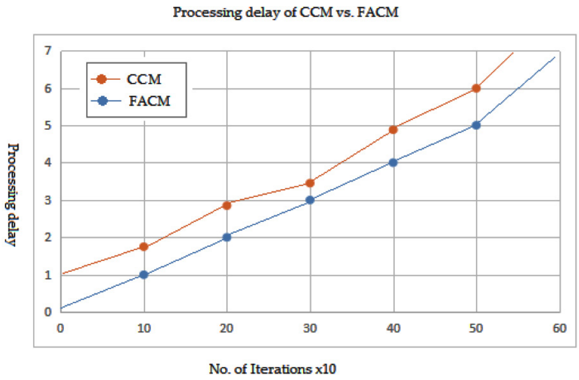

Figure 5

Processing delay of CCM vs FACM

Table 1

Comparison of existing and proposed method

S No.	References	Research Theme	Method	Quantitative Measures
1	Choi et al. 2022	Cyber physical systems protection	BOSS algorithm	Accuracy=98%, Confidence =95%
2	Aliyu et al. 2023	Path planning	Nonchalant shopper model	Speed increase 6.2%,
3	Proposed method	Fog assisted Cloud management	Wind driven optimization	Pd =52sec, latency drop = 25%,

Table 1 that presents a comparative study of existing models. In this table, you have mentioned the results and findings of various studies: Reference [14]: The study used the Boss algorithm and achieved a 98% accuracy with a 95% confidence level. Reference [15]: This study focused on a path planning system and managed to improve the speed by about 6.2%. The proposed FACM_WDO model: This model achieved a 25% reduction in latency when comparing cloud computing systems.

6. Conclusion

Dispersed processing is one among the truly astounding advancement in the state-of-the-art time frame in light of its efficiency in cost-cutting with its versatility of reducing the own resources while it fabricates the computational efficiency. Consistent assurance is expected for the present adaptable cloud conditions. The gigantic availability of cloud likewise makes irregular demonstration of weakness. Keeping these imperatives as a significant thought, the introduced framework shows up the arrangement by creating lightweight cloud climate with Mist help. Fog helped distributed computing gives a more conveyed, secure, and productive framework for handling information and conveying administrations, tending to a portion of the security challenges related with conventional cloud-driven approaches. The proposed approach thinks about the constant information assortment through edge sensor networks(ESN). the situation of information misfortune during the failing exercises, then again Fog helped cloud model (FACM) that tackle the security imperatives and recover the genuine boundaries is mimicked here. The relative examination of both the climate is basically investigated with important condition of workmanship frameworks. The system achieved 52 seconds of overall processing delay, latency drop up to 25% comparing the cloud computing model. Further the self-repairing models need to be tested in Fog environment with multiple mode of operations to test the stability on malicious activity detection.

References

[1] S.Tuli, S. Ilager, K. Ramamohanarao and R. Buyya, "Dynamic Scheduling for Stochastic Edge-Cloud Computing Environments Using A3C Learning and Residual Recurrent Neural Networks," in *IEEE Transactions on Mobile Computing*, vol. 21, no. 3, pp. 940-954, 1 March (2022), doi: 10.1109/TMC.2020.3017079.

[2] J. Son and R. Buyya, "SDCon: Integrated Control Platform for Software-Defined Clouds," in *IEEE Transactions on Parallel and Distributed Systems,* vol. 30, no. 1, pp. 230-244, 1 Jan. (2019), doi: 10.1109/TPDS.2018.2855119.

[3] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors,* vol. 19, no. 8, p. 1788 (Apr. 2019), doi: 10.3390/s19081788.

[4] M. Kahla, M. Azab and A. Mansour, "Secure, Resilient, and Self-Configuring Fog Architecture for Untrustworthy IoT Environments," 2018 17th IEEE International Conference On Trust, Security and

Privacy in Computing and Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/ BigDataSE), New York, NY, USA, pp. 49-54 (2018), doi: 10.1109/ TrustCom/BigDataSE.2018.00018.

[5] Liu, Y. Yang, K. Wang, Z. Shao and J. Zhang, "POST: Parallel Offloading of Splittable Tasks in Heterogeneous Fog Networks," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3170-3183 (April 2020), doi: 10.1109/JIOT.2020.2965566.

[6] Wu and N. Ansari, "A Cooperative Computing Strategy for Blockchain-Secured Fog Computing," in *IEEE Internet of Things Journal,* vol. 7, no. 7, pp. 6603-6609 (July 2020), doi: 10.1109/JIOT.2020.2974231.

[7] Ali, M. Adeel Pasha, S. U. Islam, H. Song and R. Buyya, "A Volunteer-Supported Fog Computing Environment for Delay-Sensitive IoT Applications," in *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3822-3830, 1 March 1 (2021), doi: 10.1109/JIOT.2020.3024823.

[8] X. Liu, W. Chen, Y. Xia and C. Yang, "SE-VFC: Secure and Efficient Outsourcing Computing in Vehicular Fog Computing," in *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3389-3399 (Sept. 2021), doi: 10.1109/TNSM.2021.3080138.

[9] S. K. Battula, S. Garg, J. Montgomery and B. Kang, "An Efficient Resource Monitoring Service for Fog Computing Environments," in *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 709-722, 1 July-Aug. (2020), doi: 10.1109/TSC.2019.2962682.

[10] Liang, M. Zhang and V. C. M. Leung, "A Reliable Trust Computing Mechanism Based on Multisource Feedback and Fog Computing in Social Sensor Cloud," in *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5481-5490 (June 2020), doi: 10.1109/JIOT.2020.2981005.

[11] C. Chiu, A. -C. Pang, W. -H. Chung and J. Zhang, "Latency-Driven Fog Cooperation Approach in Fog Radio Access Networks," in *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 698-711, 1 Sept.-Oct. (2019), doi: 10.1109/TSC.2018.2858253.

[12] Dong, S. Guo, J. Liu and Y. Yang, "Energy-Efficient Fair Cooperation Fog Computing in Mobile Edge Networks for Smart City," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7543-7554 (Oct. 2019), doi: 10.1109/JIOT.2019.2901532.

[13] M. Goudarzi, M. Palaniswami and R. Buyya, "A Distributed Deep Reinforcement Learning Technique for Application Placement in Edge

and Fog Computing Environments," in *IEEE Transactions on Mobile Computing*, vol. 22, no. 5, pp. 2491-2505, 1 May (2023), doi: 10.1109/TMC.2021.3123165.

[14] D. K. Choi, "Fog computing application of cyber-physical models of IoT devices with symbolic approximation algorithms," *J. Cloud Comput.*, vol. 11, no. 63 (2022), doi: 10.1186/s13677-022-00337-y.

[15] F. Aliyu, M. A. Abdeen, T. Sheltami, T. Alfraidi, and M. H. Ahmed, "Fog computing-assisted path planning for smart shopping," *Multimedia Tools and Applications*, vol. 82, no. 25, pp. 38827–38852 (2023).

Received April, 2025