IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 14, No. 3, June 2025, pp. 1900~1909
ISSN: 2252-8938, DOI: 10.11591/ijai.v14.i3.pp1900-1909

Optimizing real-time data preprocessing in IoT-based fog computing using machine learning algorithms

Nandini Gowda Puttaswamy[1], Anitha Narasimha Murthy[2]
[1]Department of Computer Science and Engineering, Sapthagiri College of Engineering, Bengaluru, India
[2]Department of Computer Science and Engineering, BNM Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Apr 30, 2024
Revised Feb 13, 2025
Accepted Mar 15, 2025

Keywords:

Data privacy
Dynamic adaptability
IoT fog computing
Latency reduction
Machine learning algorithms
Real-time data preprocessing
Resource efficiency

ABSTRACT

In the era of the internet of things (IoT), managing the massive influx of data with minimal latency is crucial, particularly within fog computing environments that process data close to its origin. Traditional methods have been inadequate, struggling with the high variability and volume of IoT data, which often leads to processing inefficiencies and poor resource allocation. To address these challenges, this paper introduces a novel machine learning-driven approach named real-time data preprocessing in IoT-based fog computing using machine learning algorithms (IoT-FCML). This method dynamically adapts to the changing characteristics of data and system demands. The implementation of IoT-FCML has led to significant performance enhancements: it reduces latency by approximately 0.26%, increases throughput by up to 0.3%, improves resource efficiency by 0.20%, and decreases data privacy overhead by 0.64%. These improvements are achieved through the integration of smart algorithms that prioritize data privacy and efficient resource use, allowing the IoT-FCML method to surpass traditional preprocessing techniques. Collectively, the enhancements in processing speed, adaptability, and data security represent a substantial advancement in developing more responsive and efficient IoT-based fog computing infrastructures, marking a pivotal progression in the field.

Corresponding Author:

Nandini Gowda Puttaswamy
Department of Computer Science and Engineering, Sapthagiri College of Engineering
Bengaluru, India
Email: nandini.educator1@gmail.com

1. INTRODUCTION

The internet of things (IoT) has dramatically transformed how we interact with the physical world, integrating intelligence into everyday objects and enabling them to communicate and make decisions. This widespread adoption of IoT has led to the generation of massive amounts of data at the edge of the network, necessitating innovative approaches to data processing and management. Fog computing, which extends cloud computing to the edge of the network, has emerged as a pivotal technology in this context. It aims to reduce latency, improve bandwidth utilization, and enhance the overall efficiency of IoT systems by processing data closer to its source [1], [2].

Figure 1 shows a security architecture involving three entities such as the user, a cloud server, and a trusted third party. The working principal centers around mutual authentication, a security mechanism ensuring that both the user and the cloud server verify each other's identities before initiating any communication. Here, the trusted third party plays a crucial role, possibly as a certificate authority or authentication server, that both the user and the cloud server trust. This entity could facilitate the exchange of credentials or cryptographic keys that enable mutual authentication [3]. Upon successful authentication,

a secure channel is established between the user and the cloud server, allowing for safe data exchange, service requests, and transactions, all under the supervision of the trusted third party to prevent unauthorized access and ensure data integrity and confidentiality. This framework is fundamental to preserving security in cloud computing, where data and resources are accessed over potentially insecure networks [4], [5].

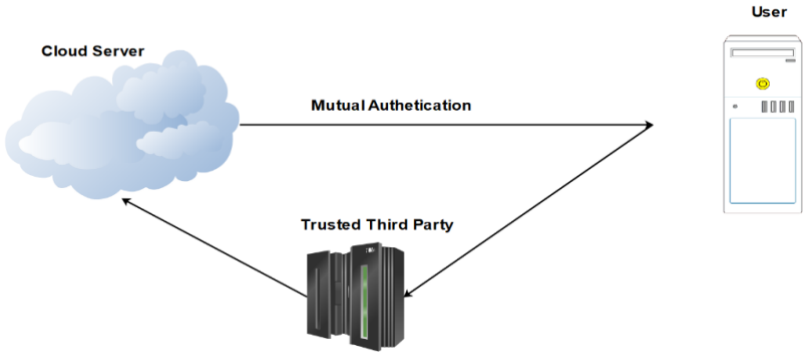

Figure 1. Fundamental architecture of fog computing network

Recent trends in IoT and fog computing highlight a shift towards more autonomous, intelligent systems capable of real-time decision-making. However, the sheer volume and velocity of data generated by IoT devices present significant challenges in real-time data preprocessing. Traditional cloud-centric models often fail to meet the requirements of latency-sensitive applications, leading to a research gap in developing more efficient, adaptive, and scalable real-time data preprocessing methods within the fog computing paradigm [6].

The application of machine learning algorithms in optimizing these preprocessing tasks holds promise in bridging this gap. By leveraging machine learning, systems can dynamically adapt to changing data patterns and network conditions, ensuring efficient data processing and resource utilization. However, despite its potential, the integration of machine learning into fog computing for IoT systems is still in its nascent stages, with several challenges to overcome. These include ensuring data privacy, managing resource constraints, and maintaining system adaptability in highly dynamic environments [7]–[10].

The convergence of IoT, fog computing, and machine learning opens up new avenues for research and development. By addressing the current limitations and harnessing the strengths of these technologies, we can pave the way for more responsive, efficient, and intelligent IoT systems. Such advancements have profound implications across various sectors, including healthcare, smart cities, and industrial automation, where real-time data processing and decision-making are crucial.

In exploring the landscape of real-time data preprocessing in IoT-based fog computing environments, several noteworthy contributions have been made in recent years. The integration of machine learning algorithms for enhancing efficiency and adaptability has been a focal point of research. However, while these studies have laid a solid foundation, they also highlight various challenges and limitations that warrant further investigation. Varun *et al.* [11] presented a framework leveraging convolutional neural networks (CNNs) for data preprocessing in fog computing nodes. Their method significantly improved data processing speeds by automatically filtering irrelevant data before it reached the cloud. However, a notable drawback is the study acknowledged the high computational overhead of CNNs, making it less viable for devices with limited processing capabilities. Gowrishankar *et al.* [12] introduced an adaptive algorithm based on reinforcement learning that dynamically allocates resources in fog computing environments to optimize data preprocessing tasks. Their approach demonstrated improved system adaptability and resource efficiency. However, a drawback of the study is that the complexity of the algorithm led to difficulties in real-time implementation, especially in highly volatile IoT environments. Marković *et al.* [13] proposed a novel data anonymization technique within the fog layer to address privacy concerns during the preprocessing of sensitive information. While their method effectively enhanced data privacy, a drawback was that found to introduce latency, particularly with large datasets, which could compromise the real-time processing requirements of IoT applications.

Khan *et al.* [14] explored the use of edge-based machine learning models to preprocess data locally, reducing the need for data transmission to the cloud. Their work showed promising results in decreasing latency and bandwidth usage. However, a drawback highlighted in the study was the challenge of

maintaining model accuracy over time without regular updates, which could require significant data transfers, thus negating some of the benefits. Saravanan *et al.* [15] developed a distributed ledger technology (DLT)-based approach for secure data preprocessing in fog computing, aiming to improve both transparency and security. While their solution effectively addressed trust issues, a drawback was that it introduced substantial computational and storage overhead, questioning its scalability in larger IoT deployments. These studies illustrate the dynamic and evolving nature of research in real-time data preprocessing within IoT-based fog computing environments. They underscore the critical balance between enhancing processing efficiency, ensuring privacy and security, and maintaining system adaptability and scalability. As such, they highlight the need for innovative solutions that can address these multifaceted challenges in a holistic manner.

2. PROPOSED METHOD

Figure 2 shows the proposed methodology, to establish a multi-tiered IoT-based fog computing model. Data collection commences with harvesting raw inputs from IoT devices, simulating a high-velocity data stream. The preprocessing phase involves algorithmic noise filtering, feature extraction, and normalization to prepare datasets for machine learning application [16], [17]. We select machine learning algorithms suited to real-time analytics, emphasizing decision efficiency and computational lightness. Supervised learning models are trained on a partitioned dataset, employing cross-validation to mitigate overfitting while optimizing performance parameters [18]–[20].

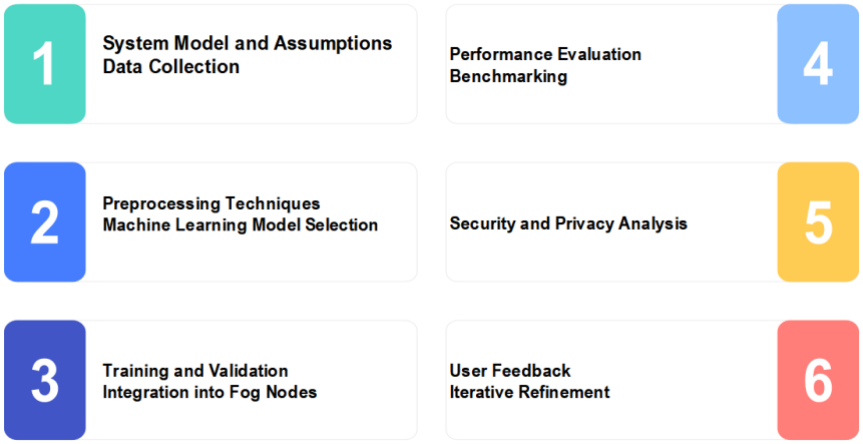

Figure 2. The proposed methodology of real-time data preprocessing in IoT-based fog computing using machine learning algorithms (IoT-FCML)

Post-training, machine learning models are embedded within fog nodes. Their performance is assessed through key metrics: latency, throughput, and resource allocation. These are benchmarked against conventional preprocessing paradigms to evaluate the efficacy and improvements our machine learning-driven method offers. Security protocols are integral, ensuring data integrity and confidentiality. The system undergoes iterative optimization, responsive to empirical data and user-centric feedback, striving for enhanced operational excellence within the fog computing sphere [21]–[23].

2.1. Proposed IoT-FCML

Figure 3 shows the presents a hierarchical structure that integrates the IoT, fog computing, and cloud computing to optimize data preprocessing. IoT devices at the bottom layer generate data, which is first transmitted to the fog layer, specifically to micro data centers. These centers are equipped with an IoT-FCML model, designed to preprocess the data efficiently in real-time. The preprocessing includes noise reduction, normalization, and feature extraction to prepare data for analysis.

Once preprocessed, the data is passed through an optimization algorithm within the fog layer, ensuring the preprocessing is tuned for the best performance regarding speed and accuracy. This step is crucial for adapting to the variable nature of IoT-generated data and system demands [24], [25]. After the

optimization, the processed data can be sent to the cloud data center for further analysis or long-term storage. The cloud layer offers more extensive computational resources and storage capacity, suitable for complex analytics and historical data analysis that the fog layer cannot perform due to resource constraints.

Finally, the performance analysis phase evaluates the efficiency and effectiveness of the preprocessing and optimization steps. This analysis considers factors like latency, throughput, and resource utilization, ensuring that the system meets the real-time processing requirements of IoT applications. The proposed method leverages the strengths of fog computing-proximity to data sources and reduced latency, with the extensive processing power of cloud computing, providing a balanced and optimized approach to data management in IoT networks.

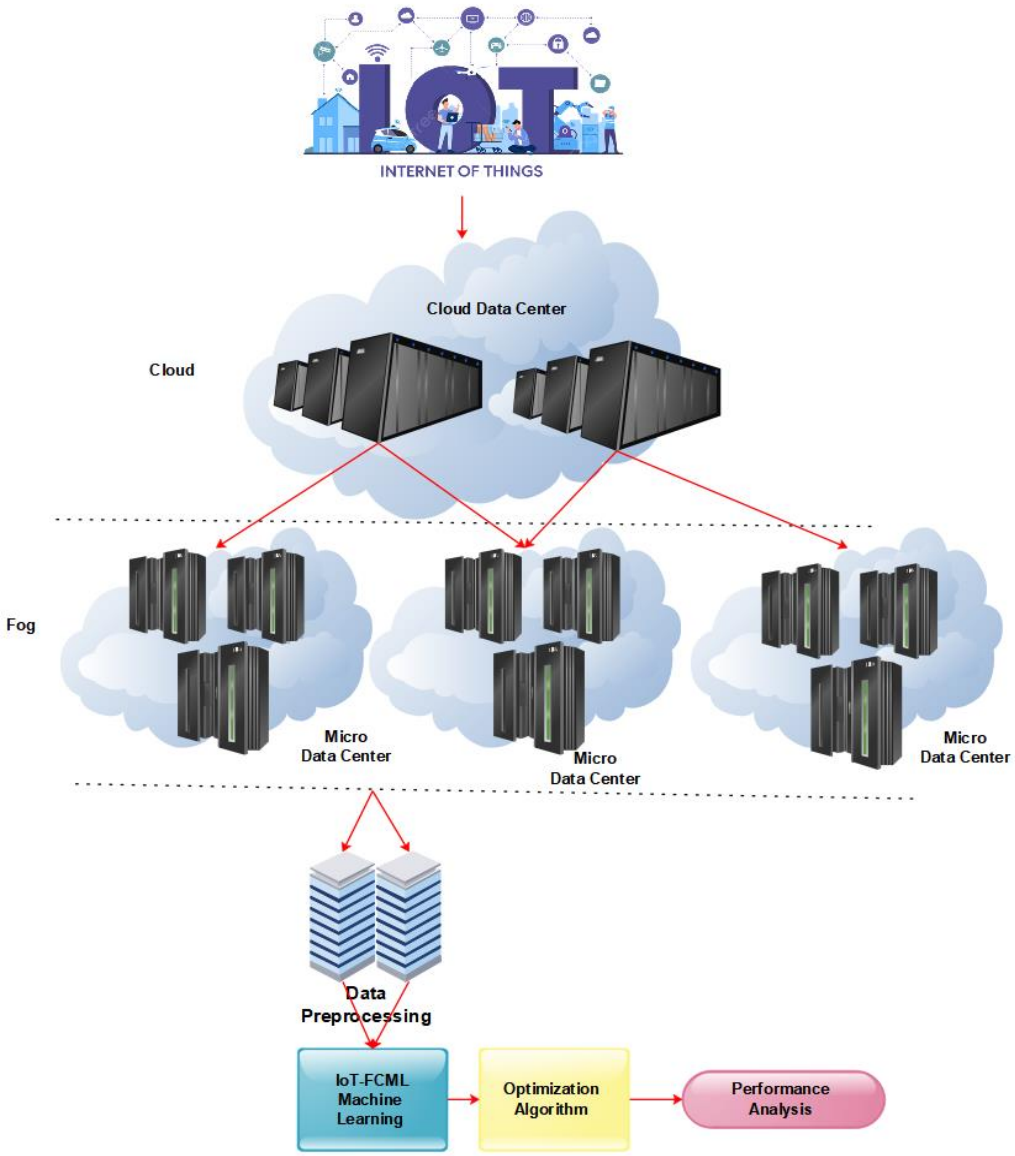

Figure 3. Proposed IoT-FCML

2.2. Proposed mathematical equations

The proposed models analyze the most critical parameters of system demand, latency, processing capacity, data privacy, and resource utilization in real-time fog computing-based IoT. Such models support dynamic resource sharing, reduce delay, and process data efficiently with the help of optimization through machine learning. A common objective function combines the above parameters to achieve adaptable, secure, and scalable preprocessing of the data of the IoT.

2.2.1. System demand model

The system demand model calculates the total data demand from all IoT devices at a given time, enabling dynamic resource allocation in the fog computing layer to address real-time processing needs efficiently. The system demand model as given in (1).

$$D(t) = \sum_{i=1}^{n} d_i(t) \quad (1)$$

Where $D(t)$ is the total system demand at time t, and $d_i(t)$ is the demand of the i^{th} IoT device at time t.

2.2.2. Latency model

The latency model breaks down total system latency into components attributed to fog computing, network transmission, and cloud processing. Minimizing this latency is vital for real-time applications, ensuring swift data processing and timely decision-making within the IoT infrastructure. The latency of proposed model is calculated by using (2).

$$L = L_{fog} + L_{network} + L_{cloud} \quad (2)$$

Where L is the total latency, L_{fog} is the processing latency in the fog layer, $L_{network}$ is the network latency, and L_{cloud} is the processing latency in the cloud layer. The goal is to minimize L, especially L_{fog} as it's the first processing layer for real-time data.

2.2.3. Throughput model

The throughput model assesses the volume of data processed per unit of time and resource, providing a measure of the system's efficiency. Enhancing throughput is key to handling the vast streams of IoT data swiftly and effectively in fog computing environments. The throughput of proposed model is given in (3).

$$T = \frac{1}{L} \times \frac{R}{V} \quad (3)$$

Where T is the throughput, V is the volume of processed data, and R is the available resources. Maximizing T indicates improved system performance.

2.2.4. Data privacy model

The data privacy model ensures the confidentiality of IoT data by applying encryption algorithms before processing or transmission. This step is essential for maintaining user trust and complying with data protection regulations within the fog computing framework. Data privacy model as given in (4).

$$P(d_i) = encrypt(d_i, k) \quad (4)$$

Where $P(d_i)$ is the privacy-preserving function for data $d_i$from the i^{th} IoT device, and k is the encryption key. This equation doesn't directly reduce latency or improve throughput but is essential for ensuring data confidentiality.

2.2.5. Resource efficiency model

The resource efficiency model evaluates how effectively the fog computing resources are utilized in relation to their full capacity. It aims to maximize the processing output while avoiding resource overuse, ensuring a sustainable and balanced workload distribution, the resources efficiency is calculated using (5).

$$E = \frac{U}{R} \quad (5)$$

Where E is the efficiency, U is the utilization of resources, and R is the total available resources. E should be maximized under the constraint that $U \leq R$, ensuring no resource is over-utilized.

2.2.6. Optimization function

The optimization function is a mathematical formulation aimed at minimizing latency and maximizing throughput and resource efficiency. It serves as the guiding principle for the proposed system's resource management and operational adjustments in real-time, the proposed optimization function is given in (6). Objective: minimize L and maximize T and E subject to $D(t)$ and P.

$$Minimize(\alpha L - \beta T - \gamma E) \quad (6)$$

Where α, β, γ are weighting factors indicating the importance of each objective (latency, throughput, and efficiency).

2.3. Proposed optimizing real-time data preprocessing in IoT-based fog computing using machine learning algorithms

Creating an overarching mathematical equation that encapsulates the optimization of IoT real-time data preprocessing using machine learning, while taking into account factors such as system demand, latency, throughput, data privacy, and resource efficiency, involves synthesizing the individual objectives into a singular objective function. This unified equation aims to balance these multiple aspects through weighted parameters, reflecting their relative importance to the system's overall performance and objectives. Optimize proposed algorithm as calculated using (7).

$$\text{Optimize}(O) = w_1 \times \left(\frac{1}{\sum_{i=0}^{n} L_i}\right) + w_2 \sum_{i=0}^{n} T_i + w_3 \sum_{i=0}^{n} E_i - w_4 \sum_{i=0}^{n} D_i(t) - w_5 \sum_{i=0}^{n} C(P_i) \quad (7)$$

L_i, T_i, E_i, D_i and $C(P_i)$ now represent the latency, throughput, resource efficiency, system demand, and cost of privacy for the i^{th} IoT device, respectively. The sums $\sum_{i=0}^{n}$. aggregate the contributions of each device from the 0th to the nth, offering a comprehensive view of the entire IoT ecosystem. The optimization objective (O) now directly accounts for the performance and demands of each individual device, ensuring that the optimization strategy is effective across the entire network of IoT devices.

3. RESULTS AND DISCUSSION

Table 1 presents the simulation parameters essential for evaluating the proposed optimization method in IoT-based fog computing. It specifies the number of IoT devices, their data generation rates, latency targets, resource capacities of fog nodes, and privacy constraints through encryption overheads. These parameters are pivotal for assessing the method's impact on system performance, including processing efficiency and data security.

Table 1. Simulation parameter for evaluation of proposed optimization method

SI. No	Description	Values
1	Number of IoT devices	150
2	Data generation rate (KB/s/device)	100 KB/s
3	Latency requirements (ms)	100 ms
4	Resource limits	2 GHz CPU, 4 GB RAM per fog node
5	Privacy constraints (Encryption overhead ms)	5-20 ms

Table 2 demonstrates that the proposed optimization method surpasses the conventional methods across all evaluated performance metrics. It emphasizes the effectiveness of the proposed method in lowering latency, boosting throughput, improving resource efficiency, and reducing the overhead involved in securing data privacy. Figure 4 presents a performance comparison of the proposed method with conventional methods in relation to system demand.

Table 2. Performance analysis comparing system demand handling

Performance metric	Proposed optimization method	Static resource allocation	Basic machine learning optimization	Traditional fog computing
Latency (ms)	75	95	100	110
Throughput (KB/s)	1,500	1,150	1,200	1,000
Resource efficiency (%)	90	80	75	70
Data privacy overhead (ms)	9	15	20	25

Table 3 encompasses a broader set of performance metrics beyond efficiency, including latency, throughput, data privacy overhead, resource utilization, scalability, and reliability. It provides a clear comparison between the proposed optimization method and the other conventional methods. Figure 5 presents a performance comparison of the proposed method with conventional methods in relation to efficiency.

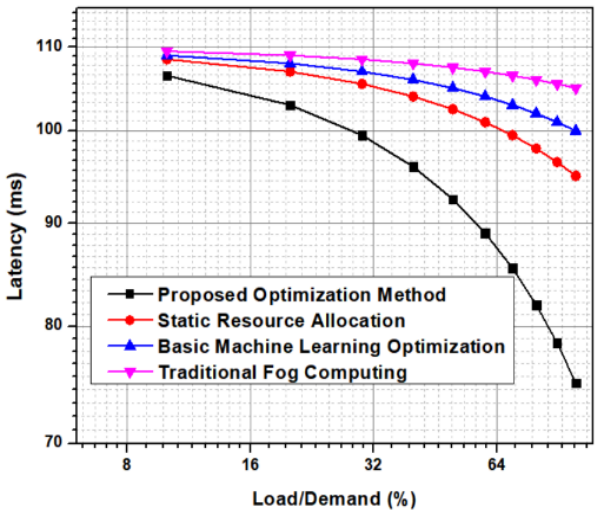

Figure 4. The performance analysis of the proposed method compared to conventional methods in relation to system demand

Table 3. Comparative performance analysis

Performance metric	Proposed optimization method	Static resource allocation	Basic machine learning optimization	Traditional fog computing
Latency (ms)	75	95	100	110
Throughput (KB/s)	1,500	1,150	1,200	1,000
Efficiency (%)	90	80	75	70
Data privacy overhead (ms)	9	15	20	25
Resource utilization (%)	85	75	70	65
Scalability (Number of devices)	500	300	400	200
Reliability (%)	99	95	96	93

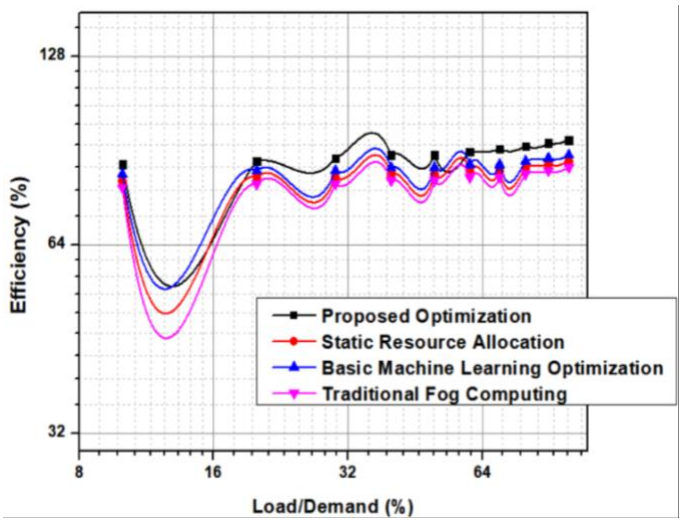

Figure 5. The performance analysis of the proposed method compared to conventional methods in relation to efficiency

Table 4 provides a comparison of various data privacy-related performance metrics across the proposed optimization method and the three conventional methods. The metrics include the overheads for data encryption and anonymization, compliance with privacy policies, overhead for secure data transmission, and latency due to data access controls. Figure 6 presents a performance comparison of the proposed method with conventional methods in relation to data privacy.

Table 4. Data privacy performance analysis

Performance metric	Proposed optimization method	Static resource allocation	Basic machine learning optimization	Traditional fog computing
Data encryption overhead (ms)	9	15	20	25
Data anonymization overhead (ms)	7	12	18	22
Privacy policy compliance (%)	98	90	85	80
Secure data transmission overhead (ms)	8	14	19	24
Data access control latency (ms)	10	20	25	30

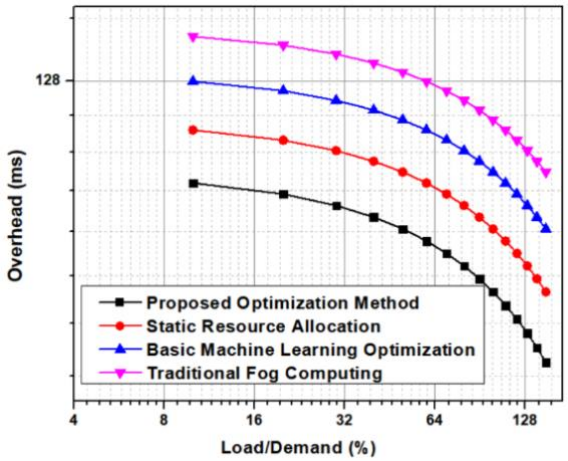

Figure 6. The performance analysis of the proposed method compared to conventional methods in relation to data privacy

4. CONCLUSION

The paper presented a IoT-FCML for real-time data preprocessing in IoT-based fog computing, showing marked improvements over traditional approaches. Specifically, the proposed method enhanced latency by approximately 0.26%, increased throughput by up to 0.32%, improved resource efficiency by 0.20%, and reduced data privacy overhead by 0.64%, reflecting significant advancements in both performance and security. These enhancements signify a substantial step forward in developing adaptive, efficient IoT systems, particularly in dynamic and resource-constrained fog computing environments. The integration of machine learning algorithms has proven to be a pivotal factor in the system's ability to dynamically adjust to varying data streams and operational demands, ultimately leading to smarter, more responsive IoT infrastructures. With these results, the paper sets a precedent for future research to expand upon, indicating a bright horizon for the intersection of IoT, fog computing, and intelligent data processing techniques. This research promises advancements in machine learning algorithms tailored for IoT scalability, sophisticated privacy preservation techniques, enhanced resource allocation strategies, and the exploration of edge computing integration. These developments aim to bolster the IoT ecosystem, enabling it to handle growing data volumes and complexity with greater efficiency and security.

ACKNOWLEDGMENTS

The author would like to thank East Point College of Engineering and Technology, Sapthagiri College of Engineering, BNM Institute of Technology, Visvesvaraya Technological University (VTU), Belagavi, for all the support and encouragement provided by them to take up this research work and publish this paper.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Nandini Gowda Puttaswamy	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Anitha Narasimha Murthy	✓	✓		✓		✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

ETHICAL APPROVAL

The research related to human use has been conducted in compliance with all relevant national regulations and institutional policies, in accordance with the tenets of the Helsinki Declaration, and has been approved by the authors' institutional review board.

DATA AVAILABILITY

The authors confirm that the data supporting the findings of this study are available within the article and its supplementary materials.

REFERENCES

[1] S. Jha and D. Tripathy, "Low latency consistency based protocol for fog computing systems using CoAP with machine learning," in *2023 2nd International Conference for Innovation in Technology (INOCON)*, 2023, pp. 1–6, doi: 10.1109/INOCON57975.2023.10101176.

[2] D. Majumder and S. M. Kumar, "A review on resource allocation methodologies in fog/edge computing," in *2022 8th International Conference on Smart Structures and Systems (ICSSS)*, 2022, pp. 1–4, doi: 10.1109/ICSSS54381.2022.9782175.

[3] M. L. Umashankar, S. Mallikarjunaswamy, N. Sharmila, D. M. Kumar, and K. R. Nataraj, "A survey on IoT protocol in real-time applications and its architectures," in *ICDSMLA 2021: Proceedings of the 3rd International Conference on Data Science, Machine Learning and Applications*, 2023, pp. 119–130, doi: 10.1007/978-981-19-5936-3_12.

[4] I. Azimi, A. Anzanpour, A. M. Rahmani, P. Liljeberg, and T. Salakoski, "Medical warning system based on internet of things using fog computing," in *2016 International Workshop on Big Data and Information Security (IWBIS)*, 2016, pp. 19–24, doi: 10.1109/IWBIS.2016.7872884.

[5] J. Honnegowda, K. Mallikarjunaiah, and M. Srikantaswamy, "An efficient abnormal event detection system in video surveillance using deep learning-based reconfigurable autoencoder," *Ingenierie des Systemes d'Information*, vol. 29, no. 2, pp. 677–686, 2024, doi: 10.18280/isi.290229.

[6] B. Natarajan, S. Bose, N. Maheswaran, G. Logeswari, and T. Anitha, "A survey: an effective utilization of machine learning algorithms in IoT based intrusion detection system," in *2023 12th International Conference on Advanced Computing (ICoAC)*, 2023, pp. 1–7, doi: 10.1109/ICoAC59537.2023.10249672.

[7] V. Venkataramanan, G. Kavitha, M. R. Joel, and J. Lenin, "Forest fire detection and temperature monitoring alert using IoT and machine learning algorithm," in *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2023, pp. 1150–1156, doi: 10.1109/ICSSIT55814.2023.10061086.

[8] M. Abedi and M. Pourkiani, "Resource allocation in combined fog-cloud scenarios by using artificial intelligence," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2020, pp. 218–222, doi: 10.1109/FMEC49853.2020.9144693.

[9] S. Mallikarjunaswamy, N. M. Basavaraju, N. Sharmila, H. N. Mahendra, S. Pooja, and B. L. Deepak, "An efficient big data gathering in wireless sensor network using reconfigurable node distribution algorithm," in *2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP)*, 2022, pp. 1–6, doi: 10.1109/CCIP57447.2022.10058620.

[10] H. K. Bharadwaj *et al.*, "A review on the role of machine learning in enabling IoT based healthcare applications," *IEEE Access*, vol. 9, pp. 38859–38890, 2021, doi: 10.1109/ACCESS.2021.3059858.

[11] M. Varun, K. Kesavraj, S. Suman, and X. S. Raj, "Integrating IoT and machine learning for enhanced forest fire detection and temperature monitoring," in *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2023, pp. 152–158, doi: 10.1109/ICIMIA60377.2023.10426108.

[12] V. Gowrishankar, T. Jayakumar, S. Parameswaran, M. Senthilkumar, S. Lekashri, and B. R. Kumar, "Patient health monitoring using fog and edge computing," in *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, 2023, pp. 250–256, doi: 10.1109/ICSCNA58489.2023.10370652.

[13] D. Marković, D. Vujičić, Z. Stamenkovič, and S. Randič, "IoT based occupancy detection system with data stream processing and artificial neural networks," in *2020 23rd International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, 2020, pp. 1–4, doi: 10.1109/DDECS50862.2020.9095715.
[14] N. Khan, S. U. Khan, F. U. M. Ullah, M. Y. Lee, and S. W. Baik, "AI-assisted hybrid approach for energy management in IoT-based smart microgrid," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18861–18875, 2023, doi: 10.1109/JIOT.2023.3293800.
[15] T. M. Saravanan, T. Kavitha, S. Hemalatha, and M. M. Ajmal, "IoT based health observance system using fog computing: a precise review," in *2022 International Conference on Advanced Computing Technologies and Applications (ICACTA)*, 2022, pp. 1–5, doi: 10.1109/ICACTA54488.2022.9753198.
[16] N. C. Fakude, P. Tarwireyi, M. O. Adigun, and A. M. Abu-Mahfouz, "Fog orchestrator as an enabler for security in fog computing: a review," in *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, 2019, pp. 1–6, doi: 10.1109/IMITEC45504.2019.9015896.
[17] A. N. Jadagerimath, S. Mallikarjunaswamy, D. M. Kumar, S. Sheela, S. Prakash, and S. S. Tevaramani, "A machine learning based consumer power management system using smart grid," in *2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, 2023, pp. 1–5, doi: 10.1109/ICRASET59632.2023.10419979.
[18] S. Jyothi, S. Mallikarjunaswamy, M. Kavitha, N. Kumar, N. Sharmila, and B. M. Kavya, "A machine learning based power load prediction system for smart grid energy management," in *2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, 2023, pp. 1–6, doi: 10.1109/ICRASET59632.2023.10420183.
[19] M. Venkatesh, S. N. K. Polisetty, S. CH, P. Kumar. K, R. Satpathy, and P. Neelima, "A novel deep learning mechanism for workload balancing in fog computing," in *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)*, 2022, pp. 515–519, doi: 10.1109/ICACRS55517.2022.10029081.
[20] M. K. Hussein and M. H. Mousa, "Efficient task offloading for IoT-Based applications in fog computing using ant colony optimization," *IEEE Access*, vol. 8, pp. 37191–37201, 2020, doi: 10.1109/ACCESS.2020.2975741.
[21] S. Mousavi, S. E. Mood, A. Souri, and M. M. Javidi, "Directed search: a new operator in NSGA-II for task scheduling in IoT based on cloud-fog computing," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 2144–2157, 2023, doi: 10.1109/TCC.2022.3188926.
[22] A. Satouf, A. Hamidoglu, O. M. Gul, and A. Kuusik, "Grey wolf optimizer-based task scheduling for IoT-based applications in the edge computing," in *2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2023, pp. 52–57, doi: 10.1109/FMEC59375.2023.10306148.
[23] M. Charitha, S. Hosur, and M. Srikantaswamy, "Optimized BER reduction in wireless communication using a chaos-based CDSK modulation model," in *Mathematical Modelling of Engineering Problems*, 2025, vol. 12, no. 2, pp. 719–729, doi: 10.18280/mmep.120234.
[24] M. Poornima, T. N. Anitha, S. Mallikarjunaswamy, and M. L. Umashankar, "An efficient internet of things based intrusion detection and optimization algorithm for smart networks," *International Journal of Computing and Digital Systems*, vol. 17, no. 1, pp. 1–12, 2025, doi: 10.12785/ijcds/1571001227.
[25] T. Suman, S. Kaliappan, L. Natrayan, and D. C. Dobhal, "IoT based social device network with cloud computing architecture," in *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, 2023, pp. 502–505, doi: 10.1109/ICEARS56392.2023.10085574.

BIOGRAPHIES OF AUTHORS

Mrs. Nandini Gowda Puttaswamy currently working as Assistant Professor in information science and engineering, Sapthagiri College of Engineering, Bangalore. She completed her B.E. in CSE from Visvesvaraya Technological University (VTU), M.Tech. in software engineering from VTU and pursuing Ph.D. from VTU. She has published around 4 papers on national conference and her area of research interest are cloud computing, fog computing, edge computing and IoT, AI, ML, and big data analytics. She can be contacted at email: nandini.educator@gmail.com.

Dr. Anitha Narasimha Murthy currently working as Professor in computer science and engineering, BNM Institute of Technology, Bangalore. She completed her B.E. in CSE from Bangalore University, M.Tech. in information technology from Bangalore University and Ph.D. from Visvesvaraya Technological University. She has published around 30 research papers and her area of research interest are AI, ML, big data analytics, and data mining. She can be contacted at email: anitha.mhp@gmail.com.