International Journal of Innovative Computer Science and IT Research

Volume 02, Issue 01 – Jan-Feb 2026 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Fog Computing Architectures for Distributed Internet of Things Applications

Enzo Mingozzi

Professor, Department of Information Engineering, University of Pisa, Italy

Abstract

The rapid expansion of Internet of Things (IoT) applications has created substantial demands for low-latency communication, distributed data processing, scalable computing, and efficient resource utilization. Conventional cloud-centric architectures often face limitations when large volumes of data are continuously generated by geographically distributed IoT devices. Fog computing addresses these limitations by extending computational, storage, and networking capabilities closer to data-producing devices. This research examines fog computing architectures designed for distributed IoT applications and analyzes their structural components, processing mechanisms, communication models, resource management strategies, and security requirements.

The study adopts a conceptual and analytical methodology based on the examination of architectural layers, distributed processing characteristics, and application requirements. Particular attention is given to device, fog, network, and cloud interactions within heterogeneous IoT environments. The analysis demonstrates that fog-based architectures can reduce communication latency, decrease unnecessary cloud traffic, support localized decision-making, and improve responsiveness for latency-sensitive IoT services. Architectural comparison further indicates that hierarchical and collaborative fog models provide greater flexibility for applications requiring geographically distributed intelligence and adaptive resource allocation.

However, challenges involving interoperability, security, scalability, mobility management, energy consumption, and dynamic resource orchestration continue to affect practical deployment. The study proposes an integrated architectural perspective in which fog nodes operate as intermediate intelligent computing entities between IoT devices and centralized cloud infrastructures. Such architectures can support real-time monitoring, smart transportation, industrial automation, healthcare monitoring, environmental sensing, and intelligent infrastructure. The findings emphasize that effective fog computing architectures require coordinated management of computing resources, communication networks, security mechanisms, and application-level requirements.

Keywords: Fog Computing, Internet of Things, Distributed Computing, Edge Intelligence, IoT Architecture, Latency Reduction, Resource Management, Cloud Computing, Network Optimization, Intelligent Systems.

1. Introduction

The Internet of Things has transformed modern computing by enabling physical objects, sensors, machines, vehicles, and embedded devices to communicate and exchange information through

interconnected networks. IoT environments continuously generate heterogeneous data that require processing, storage, analysis, and decision-making. Traditional cloud computing provides extensive computational capacity for such workloads, but transferring all IoT-generated information to centralized cloud platforms can create communication delays, bandwidth consumption, and dependency on remote data centers. These limitations become particularly significant in applications where immediate responses are required.

Fog computing has emerged as a distributed computing paradigm that extends cloud-like services toward the network edge. Rather than transmitting every data element directly to centralized cloud infrastructure, fog nodes provide intermediate processing, storage, and communication capabilities closer to IoT devices. This distributed architecture enables selected workloads to be processed locally or regionally, reducing the physical distance between data sources and computational resources. Consequently, fog computing can support applications requiring rapid response, continuous connectivity, and geographically distributed intelligence.

Distributed IoT environments are characterized by large numbers of devices operating across heterogeneous networks and physical locations. Smart cities, industrial systems, transportation networks, agricultural monitoring platforms, healthcare systems, and intelligent buildings may contain thousands or millions of interconnected devices. Managing these devices through a centralized architecture can produce bottlenecks in network communication and computational workloads. Fog architectures address this issue by distributing processing responsibilities across multiple computing layers and dynamically coordinating resources according to application requirements.

The architecture of a fog-enabled IoT system must consider several dimensions, including computational placement, communication mechanisms, resource allocation, data management, security, mobility, and service orchestration. Fog nodes may include gateways, routers, micro-data centers, access points, industrial controllers, or specialized computing devices. These nodes can perform data filtering, aggregation, preliminary analytics, event detection, and local decision-making before forwarding selected information to cloud platforms.

The objective of this research is to examine architectural models for fog computing in distributed IoT applications and evaluate their ability to support efficient, responsive, and scalable computing. The study focuses on architectural layers, resource management, communication efficiency, and security requirements. It further identifies important challenges and future research directions associated with the development of adaptive fog infrastructures for increasingly complex IoT ecosystems.

2. Objectives

2.1 Primary Objective

The primary objective of this research is to examine fog computing architectures for distributed IoT applications and evaluate how intermediate computing resources can improve latency, scalability, data processing efficiency, resource utilization, and operational responsiveness compared with conventional centralized cloud-oriented IoT architectures.

2.2 Architectural Analysis

The first objective is to analyze the structural organization of fog-enabled IoT environments by examining interactions among IoT devices, fog nodes, communication networks, and cloud platforms. The study considers how computing and storage resources can be distributed across multiple layers to

Volume 02, Issue 01 – Jan-Feb 2026 ● E-ISSN: 3067-1108 | P-ISSN: 3067-1094

support localized processing. It also examines hierarchical and collaborative architectures for heterogeneous environments where devices generate data at different rates and require different levels of computational support.

2.3 Performance and Resource Optimization

The second objective is to examine the contribution of fog computing to latency reduction, bandwidth optimization, workload distribution, and resource utilization. The study evaluates how computational tasks can be placed closer to data sources and how fog nodes can process information before cloud transmission. Efficient task allocation and dynamic resource management are considered essential for maintaining performance in large-scale distributed IoT environments.

2.4 Security and Scalability

The third objective is to identify security, interoperability, mobility, and scalability requirements associated with distributed fog architectures. As fog nodes operate across decentralized and heterogeneous environments, effective authentication, authorization, privacy protection, and secure communication are required. The study also examines how fog architectures can accommodate increasing numbers of IoT devices without creating excessive computational or communication overhead.

3. Review of Literature

3.1 Fog Computing and IoT Integration

Fog computing has been proposed as an architectural extension of cloud computing that brings computational capabilities closer to IoT data sources. Its integration with IoT enables distributed processing, local data analysis, and reduced dependency on centralized cloud infrastructures. Research in this area has emphasized that fog nodes can perform intermediate processing functions such as filtering, aggregation, caching, and event detection. This capability is especially valuable for IoT applications where continuous transmission of raw data to remote cloud servers is inefficient.

The relationship between fog computing and IoT can be understood through a layered architecture consisting of sensing devices, network infrastructure, fog nodes, and cloud platforms. Each layer performs specific computational and communication responsibilities. IoT devices generate data, fog nodes process time-sensitive workloads, and cloud systems provide large-scale storage and computational resources. This layered model creates opportunities for distributed intelligence and workload balancing across the computing continuum.

3.2 Distributed Fog Architectures

Different architectural models have been proposed to address the diversity of IoT workloads. Hierarchical fog architectures organize computing resources across multiple levels, allowing data to move between nearby and higher-level nodes according to processing requirements. Flat or collaborative architectures allow multiple fog nodes to cooperate without strict hierarchical dependencies. These approaches are suitable for environments in which computational requirements change dynamically.

Architectural flexibility is particularly important in mobile and geographically distributed IoT applications. Vehicles, mobile sensors, wearable devices, and industrial equipment may continuously change their locations or network connections. Fog architectures must therefore support dynamic node

Volume 02, Issue 01 – Jan-Feb 2026 ● E-ISSN: 3067-1108 | P-ISSN: 3067-1094

discovery, service migration, workload redistribution, and network adaptation. Such requirements have encouraged research into software-defined networking, virtualization, containerization, and intelligent orchestration mechanisms for fog environments.

3.3 Resource Management and Security

Resource management remains one of the most important issues in fog computing because fog nodes generally have fewer computational resources than centralized cloud data centers. Effective allocation of CPU capacity, memory, storage, communication bandwidth, and energy is necessary to maintain application performance. Dynamic workload scheduling can prevent overloaded fog nodes while ensuring that latency-sensitive tasks are processed locally.

Security presents another major challenge because fog infrastructures consist of distributed nodes that may be physically exposed or operated across multiple administrative domains. Authentication, secure communication, access control, data integrity, privacy protection, and intrusion detection must therefore be incorporated into architectural designs. Research increasingly considers lightweight security mechanisms and distributed trust models to protect resource-constrained IoT environments without introducing excessive processing delays.

4. Methodology

4.1 Research Design

This research adopts a conceptual and analytical research design to examine fog computing architectures for distributed IoT applications. The methodology focuses on architectural components, functional relationships, processing responsibilities, communication pathways, and resource-management requirements. A structured analytical approach is used to compare centralized cloud-oriented processing with distributed fog-enabled processing. The analysis considers latency, bandwidth utilization, scalability, computational distribution, data locality, and responsiveness as major architectural evaluation dimensions.

The study organizes the fog computing environment into interconnected layers consisting of IoT devices, communication networks, fog nodes, and cloud infrastructure. Each layer is examined according to its computational role and interaction with adjacent layers. The methodology further considers application characteristics such as workload intensity, response-time requirements, data volume, device mobility, and security sensitivity. This approach enables systematic assessment of how architectural decisions influence distributed IoT performance.

4.2 Architectural Components and Processing Model

The proposed analytical model considers four principal components: IoT devices, network connectivity, fog computing nodes, and cloud infrastructure. IoT devices generate sensor and operational data, while communication networks provide connectivity among distributed components. Fog nodes perform localized computation, data aggregation, temporary storage, and intelligent filtering. Cloud infrastructure handles computationally intensive workloads, long-term storage, global analytics, and centralized management.

The processing model follows a distributed task-placement principle. Data requiring immediate analysis are processed at nearby fog nodes, while computationally intensive or long-term analytical workloads can be transferred to cloud platforms. The model therefore avoids unnecessary transmission

of raw data and supports selective cloud communication. This architecture is intended to improve response time, reduce network congestion, and distribute computational workloads according to application requirements.

Key architectural considerations:

- Localized data processing at fog nodes
- Dynamic workload allocation
- Hierarchical resource organization
- Secure device-to-fog communication
- Fog-to-cloud coordination
- Distributed storage and caching
- Mobility-aware service management
- Fault tolerance and node availability

4.3 Performance Evaluation Framework

The performance evaluation framework considers latency, bandwidth consumption, resource utilization, scalability, reliability, and responsiveness. Latency represents the time required to process and respond to IoT requests. Bandwidth consumption reflects the volume of information transmitted toward centralized infrastructure. Resource utilization measures how effectively computational capacity is distributed among fog nodes. Scalability examines the ability of the architecture to support growing numbers of devices and workloads.

The framework also considers qualitative architectural benefits and limitations. A fog architecture is considered effective when it provides localized processing without creating excessive management complexity or security exposure. The evaluation therefore balances performance improvements against architectural overhead. Particular attention is given to distributed coordination because excessive communication among fog nodes can reduce the advantages obtained through localized processing.

4.4 Security and Resource Management Analysis

Security analysis examines authentication, authorization, encryption, integrity verification, privacy protection, and trust management across IoT, fog, and cloud layers. The distributed nature of fog infrastructure increases the number of potential attack surfaces, making security mechanisms essential at every architectural level. Lightweight security mechanisms are particularly relevant because IoT devices and fog nodes may operate under constrained computational and energy conditions.

Resource management analysis focuses on computational capacity, memory, storage, network bandwidth, and energy availability. Dynamic scheduling is considered necessary because IoT workloads can change rapidly. Effective resource orchestration should identify overloaded nodes, migrate tasks when necessary, and maintain service quality. The analysis therefore evaluates the importance of adaptive resource allocation for sustaining stable performance in large-scale distributed fog environments.

5. Analysis

5.1 Comparison of Cloud-Centric and Fog-Enabled IoT Architectures

Cloud-centric IoT architectures typically transmit substantial amounts of device-generated data to centralized cloud infrastructure. Although this approach provides powerful computational resources, continuous remote processing can introduce communication latency and increased network traffic. Fog computing distributes selected processing activities across intermediate nodes, allowing time-sensitive workloads to remain closer to the data source. The architectural comparison below summarizes major characteristics of centralized cloud processing and fog-enabled IoT processing.

Table 1: Comparative Characteristics of Cloud-Centric and Fog-Enabled IoT Architectures

Evaluation Dimension	Cloud-Centric IoT	Fog-Enabled IoT
Data Processing Location	Centralized cloud	Distributed across fog and cloud
Response Latency	Relatively higher	Relatively lower
Bandwidth Demand	High	Reduced through local processing
Data Locality	Limited	High
Real-Time Processing	Moderately suitable	Highly suitable
Resource Distribution	Centralized	Distributed
Scalability	High cloud capacity	High through layered distribution
Local Decision-Making	Limited	Strong
Mobility Support	Dependent on network architecture	Better through distributed nodes
Network Congestion	Higher potential	Lower potential
Fault Isolation	More centralized	Distributed
Application Responsiveness	Moderate	High

Interpretation: Table 1 indicates that fog-enabled architectures provide important advantages for applications requiring low latency and localized decision-making. By processing information closer to IoT devices, fog systems can reduce unnecessary data transmission and improve responsiveness. Cloud computing remains valuable for large-scale storage and computationally intensive workloads, indicating that fog and cloud should generally operate as complementary layers rather than competing infrastructures.

5.2 Fog Resource Distribution and Application Performance

The performance of fog-enabled IoT applications depends heavily on the appropriate distribution of computational workloads. Processing all workloads at a single fog node may create resource bottlenecks, whereas excessive communication between multiple fog nodes can generate coordination overhead. Effective architectures therefore require workload-aware scheduling and dynamic task allocation.

Applications such as industrial automation, intelligent transportation, healthcare monitoring, and smart surveillance benefit particularly from localized processing. In these applications, decisions may need to be generated within milliseconds or seconds. Fog nodes can analyze sensor information locally and forward only relevant information to cloud infrastructure, thereby improving response time and reducing unnecessary network traffic.

Table 2: Major Fog Architecture Requirements for Distributed IoT Applications

Requirement	Architectural Function	Expected Benefit
Low-Latency Processing	Local computation	Faster responses
Dynamic Resource Allocation	Adaptive workload placement	Improved utilization
Data Filtering	Local preprocessing	Reduced bandwidth usage
Edge/Fog Collaboration	Distributed coordination	Better workload distribution
Secure Authentication	Device and node verification	Improved security
Data Encryption	Protection during transmission/storage	Enhanced privacy
Service Migration	Movement of workloads between nodes	Mobility support
Fault Tolerance	Recovery from node failures	Higher reliability
Virtualization	Flexible resource provisioning	Improved scalability
Cloud Integration	Long-term analytics and storage	Expanded computational capability

Interpretation: Table 2 demonstrates that effective fog architectures require more than localized computation. They need coordinated resource allocation, secure communication, service migration, fault tolerance, and cloud integration. These capabilities allow fog infrastructure to support dynamic IoT workloads while preserving scalability and reliability. The combination of localized and centralized processing provides a balanced computing model for heterogeneous distributed applications.

Volume 02, Issue 01 – Jan-Feb 2026 ● E-ISSN: 3067-1108 | P-ISSN: 3067-1094

5.3 Architectural Implications

The analysis indicates that fog computing can transform IoT environments from predominantly centralized data-processing systems into distributed intelligent computing ecosystems. The primary architectural advantage arises from computational proximity. When processing occurs close to data-generating devices, applications can respond more rapidly and reduce the amount of information transmitted through core networks.

However, distributed architecture also increases management complexity. Multiple fog nodes must be monitored, authenticated, configured, and coordinated. Resource availability can vary significantly across nodes, and failures may occur independently. Consequently, future fog architectures should incorporate automated orchestration, intelligent workload prediction, adaptive security, and self-healing mechanisms to maintain stable service performance.

6. Discussion

6.1 Distributed Intelligence in IoT

Fog computing provides a practical foundation for distributed intelligence in IoT environments. Rather than relying entirely on remote cloud servers, applications can perform localized analytics at fog nodes. This arrangement is particularly beneficial for systems that continuously generate high-frequency sensor information. Local processing can identify relevant events and reduce the need to transmit complete datasets to centralized infrastructure.

Distributed intelligence also enables context-sensitive decision-making. Fog nodes can combine information from nearby sensors and devices to understand local conditions. This capability supports applications such as traffic management, industrial monitoring, environmental sensing, and smart infrastructure. The architecture therefore improves not only processing efficiency but also the responsiveness and contextual awareness of IoT services.

6.2 Resource and Service Management

Efficient resource management is essential because fog nodes differ in processing capacity, memory, storage, connectivity, and energy availability. Static workload assignment may lead to inefficient utilization or overloaded nodes. Dynamic orchestration mechanisms can instead distribute workloads according to current resource conditions and application requirements.

Containerization, virtualization, and software-defined infrastructure can further improve flexibility. These technologies allow applications to be deployed, migrated, and scaled across fog nodes without requiring significant hardware modifications. Intelligent orchestration can therefore provide adaptive service placement while maintaining application-level performance requirements.

6.3 Security and Reliability

Fog computing expands the security boundary beyond centralized cloud infrastructure. Fog nodes may operate in public, industrial, residential, or mobile environments and may therefore face physical and cyber threats. Secure identity management, encrypted communication, access control, and anomaly detection should be implemented throughout the computing hierarchy.

Reliability also requires distributed fault management. If a fog node becomes unavailable, workloads should be transferred to another suitable node or cloud infrastructure. Such mechanisms can

prevent localized failures from disrupting complete IoT services. Consequently, security and reliability must be treated as fundamental architectural components rather than additional features.

7. Challenges

Fog computing architectures face significant scalability challenges because IoT environments may contain thousands or millions of heterogeneous devices. As the number of devices increases, fog infrastructure must dynamically manage computing resources, communication connections, service requests, and security policies. Limited fog-node capacity can produce resource contention when multiple applications compete for processing resources. Effective orchestration mechanisms are therefore required to distribute workloads intelligently while avoiding excessive coordination overhead among geographically distributed nodes.

Security and privacy represent another major challenge. Fog nodes are distributed closer to physical environments and may therefore be more exposed to unauthorized access, device compromise, malicious workloads, and network attacks. The large number of communication relationships among devices, fog nodes, and cloud systems increases the complexity of identity management and access control. Lightweight but strong security mechanisms are required to protect sensitive information without imposing excessive computational overhead.

Interoperability and mobility create additional architectural difficulties. IoT devices frequently use different communication technologies, operating systems, data formats, and application protocols. Integrating these heterogeneous components into a unified fog environment requires standardized interfaces and adaptive communication mechanisms. Furthermore, mobile devices and vehicles may change their network attachment points frequently, requiring dynamic service migration and resource reallocation. These factors make static fog architectures unsuitable for highly dynamic IoT environments.

8. Future Research

Future research should investigate artificial intelligence-driven orchestration mechanisms capable of predicting IoT workloads and automatically allocating fog resources. Machine learning models could estimate demand, identify potential resource bottlenecks, and determine optimal task placement. Such mechanisms could enable fog infrastructures to adapt continuously to changing application requirements.

Research should also examine lightweight learning models suitable for resource-constrained fog environments so that intelligent management does not create substantial computational overhead. Another important direction involves decentralized security and privacy mechanisms. Blockchain-based trust models, distributed identity management, and intelligent intrusion detection could strengthen communication among IoT devices and fog nodes. Future architectures should investigate privacy-preserving analytics that allow useful information to be extracted without exposing sensitive raw data. Secure federated learning may also provide opportunities for collaborative intelligence across distributed fog environments while reducing direct data sharing.

Future studies should further explore integrated fog-edge-cloud computing models. Rather than treating fog, edge, and cloud infrastructures as isolated environments, researchers can develop unified computing continua in which workloads dynamically move according to latency, resource availability, energy consumption, and application priorities. Digital twins, autonomous orchestration, network

Volume 02, Issue 01 – Jan-Feb 2026 ● E-ISSN: 3067-1108 | P-ISSN: 3067-1094

slicing, and intent-based networking may provide additional capabilities for future distributed IoT infrastructures. Experimental testbeds and large-scale real-world deployments will also be important for validating architectural models under realistic workloads.

9. Conclusion

Fog computing provides an important architectural solution for addressing the limitations of centralized cloud-oriented processing in distributed Internet of Things environments. The continuous growth of IoT devices has increased the volume, velocity, and heterogeneity of generated data, creating significant demands for low-latency processing, efficient bandwidth utilization, localized intelligence, and scalable resource management. The analysis presented in this study demonstrates that fog computing can extend computational capabilities toward IoT data sources by introducing intermediate processing layers between devices and centralized cloud infrastructure. This distributed approach allows time-sensitive workloads to be processed closer to their origin while computationally intensive and long-term workloads can continue to benefit from cloud resources. Consequently, fog computing can improve responsiveness, reduce unnecessary communication, and support more efficient use of distributed computing resources.

The study also demonstrates that successful fog computing architectures require coordinated management of multiple architectural components. IoT devices, communication networks, fog nodes, and cloud platforms must operate as interconnected layers rather than independent systems. Dynamic task placement, resource allocation, data filtering, service migration, fault tolerance, and secure communication are essential for maintaining reliable performance. Hierarchical and collaborative fog models can provide flexible mechanisms for distributing workloads across geographically dispersed environments. At the same time, the decentralized nature of fog computing introduces challenges related to security, interoperability, scalability, mobility, and administrative complexity. These challenges indicate that fog architecture design must balance computational proximity with coordination overhead, resource limitations, and security requirements. The analysis further suggests that fog and cloud computing should be considered complementary components within an integrated computing continuum.

Future development of fog-enabled IoT systems should therefore focus on intelligent orchestration, adaptive resource management, decentralized security, privacy-preserving analytics, and seamless fog-edge-cloud integration. Artificial intelligence can provide predictive mechanisms for workload placement and resource optimization, while virtualization and containerization can improve application mobility and service scalability. Secure distributed identity systems and intelligent anomaly detection can strengthen the protection of geographically distributed infrastructure. As IoT applications increasingly support smart cities, industrial automation, intelligent transportation, healthcare, environmental monitoring, and other real-time services, fog computing can become a critical foundation for distributed digital intelligence. Overall, the adoption of well-designed fog computing architectures can enable IoT ecosystems to become more responsive, scalable, secure, and computationally efficient.

References

1. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*, 13–16. https://doi.org/10.1145/2342509.2342513
2. Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal, 3*(6), 854–864. https://doi.org/10.1109/JIOT.2016.2584538
3. Stojmenovic, I., & Wen, S. (2014). The fog computing paradigm: Scenarios and security issues. *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, 1–8. https://doi.org/10.15439/2014F503
4. Yi, S., Li, C., & Li, Q. (2015). A survey of fog computing: Concepts, applications and issues. *Proceedings of the 2015 Workshop on Mobile Big Data*, 37–42. https://doi.org/10.1145/2757384.2757397
5. Naha, R. K., Garg, S., Georgakopoulos, D., Jayaraman, P. P., Gao, L., Xiang, Y., & Ranjan, R. (2018). Fog computing: Survey of trends, architectures, requirements, and research directions. *IEEE Access, 6*, 47980–48009. https://doi.org/10.1109/ACCESS.2018.2866491
6. Mukherjee, M., Shu, L., & Wang, D. (2018). Survey of fog computing: Fundamental, network applications, and research challenges. *IEEE Communications Surveys & Tutorials, 20*(3), 1826–1857. https://doi.org/10.1109/COMST.2018.2814571
7. Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the Internet of Things: A review. *Big Data and Cognitive Computing, 2*(2), 10. https://doi.org/10.3390/bdcc2020010
8. Puliafito, C., Mingozzi, E., Longo, F., Puliafito, A., & Rana, O. (2019). Fog computing for the Internet of Things: A survey. *ACM Transactions on Internet Technology, 19*(2), Article 18. https://doi.org/10.1145/3301443
9. Bellavista, P., Berrocal, J., Corradi, A., Das, S. K., Foschini, L., & Zanni, A. (2019). A survey on fog computing for the Internet of Things. *Pervasive and Mobile Computing, 52*, 71–99. https://doi.org/10.1016/j.pmcj.2018.12.007
10. Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., Kong, J., & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture, 98*, 289–330. https://doi.org/10.1016/j.sysarc.2019.02.009
11. Peng, L., Dhaini, A. R., & Ho, P.-H. (2018). Toward integrated Cloud–Fog networks for efficient IoT provisioning: Key challenges and solutions. *Future Generation Computer Systems, 88*, 606–613.
12. Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., & Leon-Garcia, A. (2020). Fog computing: A comprehensive architectural survey. *IEEE Access, 8*, 69105–69133. https://doi.org/10.1109/ACCESS.2020.2983253
13. Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., Morrow, M. J., & Polakos, P. A. (2018). A comprehensive survey on fog computing: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials, 20*(1), 416–454. https://doi.org/10.1109/COMST.2017.2771153
14. Rahmani, A. M., Liljeberg, P., Preden, J. S., & Jantsch, A. (Eds.). (2018). *Fog computing in the Internet of Things: Intelligence at the edge*. Springer.

15. Mäkitalo, N., Ometov, A., Kannisto, J., Andreev, S., Koucheryavy, Y., & Mikkonen, T. (2018). Architecting the Web of Things for the fog computing era. *IET Software, 12*(5), 381–389. https://doi.org/10.1049/iet-sen.2017.0350
16. Singh, J., Singh, P., & Gill, S. S. (2021). Fog computing: A taxonomy, systematic review, current trends and research challenges. *Journal of Parallel and Distributed Computing, 157*, 56–85. https://doi.org/10.1016/j.jpdc.2021.06.005
17. Laroui, M., Nour, B., Moungla, H., Cherif, M. A., Afifi, H., & Guizani, M. (2021). Edge and fog computing for IoT: A survey on current research activities & future directions. *Computer Communications, 180*, 210–231. https://doi.org/10.1016/j.comcom.2021.09.003
18. Martinez, I., Senhaji Hafid, A., & Jarray, A. (2021). Design, resource management, and evaluation of fog computing systems: A survey. *IEEE Internet of Things Journal*, *8*(4), 2494–2516. https://doi.org/10.1109/JIOT.2020.3022699
19. *The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications*. (2020). *Internet of Things, 9*, 100177. https://doi.org/10.1016/j.iot.2020.100177
20. Naha, R. K., Garg, S., Georgakopoulos, D., Jayaraman, P. P., Gao, L., Xiang, Y., & Ranjan, R. (2018). Fog computing architecture: Survey and challenges. In *Fog computing: Concepts, frameworks and applications* (pp. 1–20). Springer.