iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IX **Month of publication:** September 2026

DOI: https://doi.org/10.22214/ijraset.2026.84840

Edge Computing Landscapes: A Comprehensive Taxonomy and State-of-the-Art Analysis

Dr. Meena Kumari, Dr. Rajesh Verma, Mr. Naveen Monga
[1]*Assistant Professor (Computer Science),* [2, 3]*Associate Professor (Computer Science), Pt. C.L.S. Govt. College, Karnal, Haryana*

Abstract: The needs of scenarios such as the rapidly expanding Internet of Things (IoT) ecosystem or real-time services are examples of situations where a centralized cloud model may not suffice, as all data resides on the cloud and traditional cloud computing practices have limitations. Low latency, high bandwidth and privacy issues arise due to the ever-growing amount of data being generated by connected devices. One way to address these issues is to move computation, storage and networking resources closer to the edge where data is generated. Edge computing can minimize latency in latency-sensitive applications and can also help reduce network congestion by offloading processing from the core network. This paper surveys the recent works in edge computing, classifying the existing body of work in edge computing into four categories based on four dimensions: physical architecture, algorithmic optimization techniques, performance objectives, and security mechanisms. The survey provides examples of representative works for each dimension, analyses the corresponding performance-energy trade-offs based on processing performance, energy consumption, and security objectives, and presents future research challenges such as hardware heterogeneity, network dynamics, and the development of energy-efficient edge systems. The paper also outlines research directions to enable the development and deployment of cloud-to-edge and cloud-to-thing computing environments in the future.
Keywords: Cloud Computing, Mist Computing, Fog Computing, Edge Computing.

I. INTRODUCTION

The networking edge has become a major source of large quantities of data due to such increased IoT (Internet of Things) deployments, smart infrastructure and high-fidelity streaming services. In fact, the most common architectural paradigm for years has been based on centralized cloud computing infrastructures that ingested, stored, and processed this data. Yet routing huge, high-throughput data streams globally across WAN to hyperscale cloud data centers some distance apart represents the worst systemic bottleneck of them all. Latency from end to end is high, network jitter is un predictable; and backhaul bandwidth utilization by the thousands of sensors, tracker, or edge node repeatedly becomes a bottleneck [21]. Edge computing has emerged as a critical computing paradigm designed to solve these architectural limitations by shifting computational power, storage, and networking resources directly to the data generation source [2, 27].

While edge computing does provide for the privacy preservation and the minimization of latency, the orchestration of resources within this environment is very complex. The environment includes nodes with heterogeneous hardware, links between these nodes that fluctuate in quality and nodes with limited resources [22]. As a result, the structuring and securing of these environments is an area of research in computing [18]. This survey is designed to provide a unified structure for guiding those who are intending to perform research in this area. The primary contributions of this survey paper are threefold:

1) Quadrant Classification of Edge Computing: The research provides a comprehensive classification system that looks at four dimensions of edge computing including its location, optimization approaches, objectives, and security features within the whole ecosystem.
2) Analysis of Literature References Post-2018: The analysis of prior investigations is conducted in a sequential manner by the study to show the evolution of the field over the time.
3) Identifying the Future Directions: The paper mentions the unresolved engineering requirements regarding hardware level differences, mobile participants in the system, and security costs/benefits and provides recommendations for future research on the topic.

The rest of this paper is organized as follows. Section II introduces the background concepts and discusses the structural boundaries of the computing continuum. Section III presents the proposed multi-dimensional taxonomy framework along with its corresponding architectural representation. Section IV provides a comprehensive thematic review of the literature, offering an in-depth analysis of selected studies organized according to the proposed taxonomy.

Section V presents a comparative discussion using a master evaluation matrix to examine the key trade-offs among latency, energy efficiency, and security overhead. Section VI highlights the major open research challenges and outlines promising directions for future work. Finally, Section VII concludes the paper by summarizing the key findings and contributions of this study.

II. BACKGROUND CONCEPTS AND THE COMPUTING CONTINUUM

To understand the technical literature on edge computing, it should be viewed as part of a wider computing continuum instead of a standalone technology. In many reviews, terms such as edge, fog, and mist computing are frequently used interchangeably, which can cause confusion [21–23]. This section illuminates their structural hierarchy (Fig. 1) and demonstrates how data flows from end devices through intermediate layers to the centralized cloud.

A. Mapping the Structural Landscape (Cloud, IoT, Fog, and Mist)

1) Internet of Things (IoT) vs. Edge Computing: The Internet of Things, as a source of physical-world data, consists of millions of interconnected sensors, cameras, and actuators that collect telemetry data from real-world scenarios; traditional IoT systems can only generate data, and lack sufficient storage and computing power [30], while edge computing, acting as their core "brain", enables local real-time processing without relying on cloud infrastructure.
2) Mist Computing vs. Edge Computing Mist computing lives at the very edge of the computing world, where it works as a small, lightweight part of edge computing. It means the IoT device handles the data right on its own chips and built-in microcontrollers, rather than sending everything to Cloud [21]. In contrast, edge computing runs on bigger nearby devices, placed just outside the sensor, with enough power to run small virtualization containers or neural networks.
3) Fog Computing vs. Edge computing: Both are closely linked, but they work at different levels and differs in size and structure. Fog computing is an extension of the cloud computing paradigm that brings computing and storage resources closer to where data is generated, operating at the regional network level with interconnected devices such as base stations, routers, and switches to form an intermediate infrastructure layer between end devices and the cloud [22]. On the other hand, edge computing aims to run applications as close to individual devices as possible, often on nearby gateways or local controllers, to facilitate low-latency and device-specific operations [24,30].

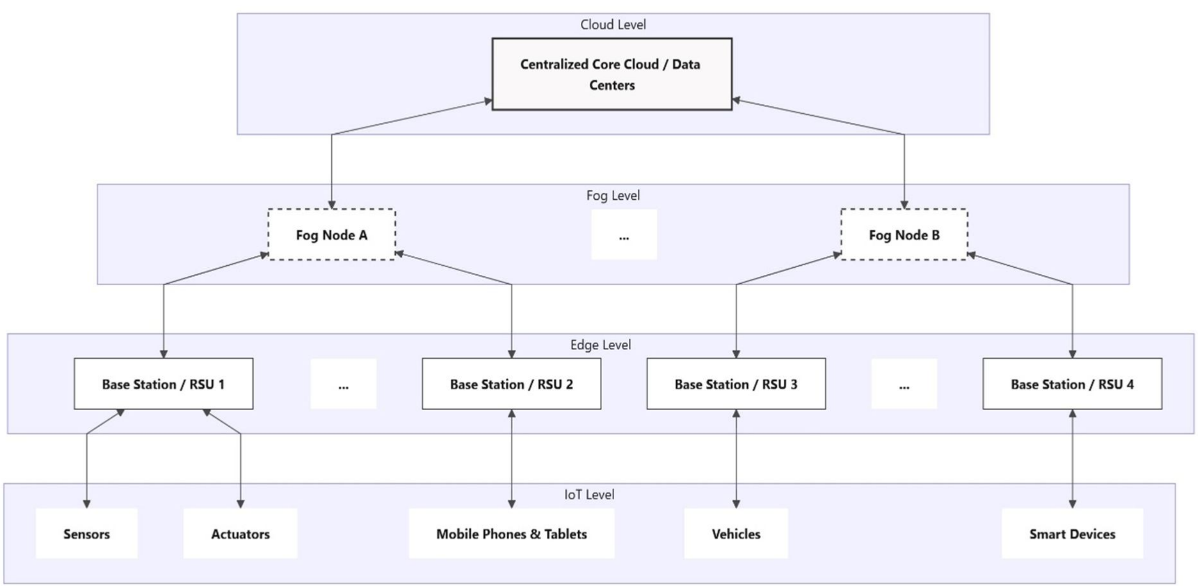

Fig 1: Computing Continuum

4) Cloud Computing vs. Edge Computing: Cloud computing is characterized by centralized data centers with enormous, almost vast computing and storage potential [23] whereas the edge computing is befitted for tasks that entail low latency, are real-time, and have restricted complexity. The Cloud trains large machine learning models, scrutinizes long-term trends, and orchestrates everything across networks [26].

B. Shifting from a Physical Continuum to an Analytical Literature Taxonomy

Transitioning from mapping the network's physical layout to examining its technical literature, it requires a major reorientation of perspective. No one can evaluate an edge network just by its hardware alone [25]. Even if physical computing resources reveal how information perpetuates through real devices, one cannot assess a network by considering the fact that where its servers are located.

To build or study an existent edge system, a researcher must address numerous aspects concurrently. For instance, when information goes from a tangible IoT sensor to an adjoining edge gateway, it's more than just moving from one place to another. It swiftly spurs three clear research queries: which intelligent algorithm should route the incoming data? Which objective should be prioritized, such as energy conservation or performance improvement? How do they safeguard that wireless data stream from hackers? Therefore, the physical continuum mentioned in the receding sections acts as the spatial framework of the network, but the technical literature must be supported by the operational software logic, before this framework can truly come to life.

Rather than just looking at the hardware alone, this paper uses a four-axis methodology to show how design choices in the hardware shapes algorithm decisions and finally determine the system's security level. This is the solid motivation behind the common taxonomy framework this paper explains in the following sections.

III. STRUCTURAL TAXONOMY FOR EDGE COMPUTING PARADIGMS

This paper puts a strong groundwork for the literature review by categorizing current Edge Computing research papers into a well-defined, multi-dimensional taxonomy. This paper presented the research papers into four key areas namely Architectural design (Table 1) i.e. how hardware is set up, Algorithmic Optimization methodologies i.e., how algorithms are improved, System Objectives i.e. what the system is built to achieve and cryptographic security i.e. how cryptography keeps everything secure.

Table 1: Edge Computing State-of-the-art Survey

Architectural Design	Algorithmic Optimization	System Objectives	Security & Privacy
Far Edge	Heuristics & Mathematical Scheduling	Latency Minimization	Encryption & Lightweight Cryptography
Near Edge	Statistical Machine Learning	Energy Efficiency	Authentication, Trust Management & Decentralized Identity
Cloudlet Layer	Deep Reinforcement Learning	Bandwidth Preservation	Hardware Security & Tamper Resistance
Multi-Tier Continuum	Game-Theoretic Resource Allocation	Cost Minimization	

A. Spatial Topologies and Architectural Tiers

The location of Edge resources suggests how quickly and how well these resources work. The nearer they are to the user, the better will be the performance. This particular dimension shows where data is processed, physically and logically, while it moves across the network path. By considering this dimension, one can track their data as they move from small devices to adjacent hubs, and even to adjoining cellular towers. By grouping research based on physical location, from the outer edge to layered systems, we can clearly see that physical location shapes how long delays last and how much data the network can handle [22].

It shows how data processing happens in the network, starting at the nearest data sources and working outward to remote systems and infrastructure [28]. On the outermost edge, the Far Edge runs tasks right where they're needed, even on low-power IoT sensors, smart appliances, and nearby devices. As we move one step inside, the Near Edge gathers data and checks traffic using local gateways, smart routers, and regional access points. For bigger computing needs, the Cloudlet Layer sets up nearby mini data centers and cell towers, so processing stays cloud-fast within a few milliseconds. At last, the Multi-Tier/Core Cloud ties everything together, moving work between nearby edge devices and faraway cloud servers as network conditions change.

This review looks at how different building designs handle these physical limits. Shi et al. [1] proposed a base architecture to help define these boundaries. It clearly delineates the operational boundaries and data interfaces between decentralized edge processing elements and remote hyperscale cloud data centres. It clearly sets the limits and explains how data should move between edge devices and distant big cloud data centers.

Mouradian et al. [2] formalize a hierarchical model for intermediate processing layers, analysing how regional smart gateways and local routers aggregate and filter data traffic before it reaches the core network. Build a clear hierarchical framework for intermediate layers, and study how regional smart gateways and local routers gather, sort, and screen data traffic before it enters the main core network.

Mach and Becvar [3] explored how to bring multi-access edge computing (MEC) into mobile cellular networks. They study where to place virtual micro-clouds, specifically putting them inside base stations. Lu et al. [4] explored vertically integrated, multi-tier network topologies that require continuous synchronization and dynamic workload partitioning across a collaborative device-edge-cloud continuum. Finally, targeting the most resource-scarce environments, Martinez et al. [5] evaluate embedded systems and microcontrollers located at the absolute perimeter of the network, optimizing how raw sensor data is parsed locally under strict hardware limitations.

B. Technical and Algorithmic Optimization Methodologies

Managing, sending data, and scheduling tasks over a spread-out network takes smart software to manage it. This dimension focuses on the automated decision-making tools that handle these complex operations. Because edge networks change rapidly and behave in unpredictable ways, rigid fixed rules fail in practice, so researchers have to explore many different mathematical algorithms. These include everything from simple fast calculations and predictive AI to self-learning reinforcement agents and models built on game theory [30]. Recent studies have examined decentralized approaches such as federated learning, which allow nearby devices to adapt to varying conditions without sharing private data. This section shows how different algorithms help edge networks make quick, smart choices even when conditions are volatile and unpredictable.

Controlling and directing computational tasks across complex edge networks requires advanced algorithmic designs. In order to address the state-of-the-art problems, Deng et al. [6] evaluated model-free, multi-agent deep reinforcement learning techniques designed to handle real-time network state changes autonomously. Aslanpour et al. [7] proposed a fast-mathematical heuristic scheduling algorithm, which demonstrated how low-overhead approximations can efficiently map tasks across heterogeneous edge layers without computational lag.

When various independent devices have to share the same group of edge resources, Rawat and Parwez [8] deployed game-theory-based optimization models using Nash equilibrium to fairly distribute network resources and avoid congestion. In order to make these networks anticipate problems instead of merely reacting, Dinh et al. [9] has integrated traditional machine learning algorithms with workload forecasting models, enabling systems to pre-emptively offload tasks before real-time bottlenecks appear. Zhou et al. [10] had explored the paradigm of edge intelligence and federated learning, which investigated how neural networks can learn on local devices without impacting user privacy.

C. Systemic Performance Objectives

Every Edge Computing system begin with clear goals and make trade-offs, so prioritising one measure higher may adversely affect another performance measure. Studies in this paper are arranged in terms of the main aim they choose to optimize. A setup built to run fast and with strict deadlines will likely empty a smartphone battery in no time. Conversely, a setup meant to save power or reduce data will often add tiny processing delays. System designers have to weigh reliable performance against hosting costs and the environmental impacts of keeping them under execution [30]. This paper scrutinises different research approaches dealing with those competing priorities.

Every edge computing setup must balance strict technical trade-offs tied to its primary goal. In systems where safety is critical, Zhang et al. [11] focused entirely on latency minimization and strict deadline enforcement, optimizing task delivery paths for real-time applications where data delay is unacceptable. On the other hand, for portable and mobile edge setups, You and Huang [12] focused on saving energy when offloading tasks, designing resource rules to cut battery use and make devices last longer. Luan et al. [13] investigated bandwidth-aware data compression and localized caching strategies designed to curtail data inflation and lower backhaul traffic loads.

From a financial perspective, Wang et al. [14] analysed cost-effective micro-cloud provisioning, developing economic allocation models that optimize the balance between operational infrastructure expenditures and user service agreements. Finally, viewing the domain through an environmental lens, Shafique et al. [15] explore green edge computing architectures, reviewing sustainable methodologies like thermal-aware resource management to lower the carbon footprint of massive distributed networks.

D. Security and Privacy Domains

Edge equipment spread across public areas leaves cloud data centers vulnerable to security issues. The final category measures whether protection systems and encryption frameworks actually preserve information integrity and user data privacy on shared networks. Since these public edge nodes often get overlooked, they face a wide range of threats, from eavesdropping on wireless signals to outright hijacking of the hardware. This dimension reviews current protection techniques and explains how researchers adapt to the tight energy and computing constraints of edge devices with tools such as lightweight encryption, decentralized identity checks, hardware-based isolation, and blockchain records [20].

To map this landscape, Xiao et al. [16] presented a comprehensive evaluation of security threats associated with multi-tenant edge ecosystems, categorizing malicious patterns from data breaches to node spoofing. They offered a thorough review of threats specific to shared edge environments, grouping harmful activity ranging from data theft to fake nodes. Al-Turjman [17] looked at networks built from low-power devices and studied light encryption methods, highlighting symmetric systems that keep data safe without overloading small IoT devices.

Sun et al. [18] evaluated decentralized authentication and access control frameworks, showing how mutual trust can be verified instantly without depending on a centralized cloud server. Khan et al. [19] examined hardware security modules and Trusted Execution Environments (TEEs), establishing hardware-level boundations to avert physical data tampering at unattended edge resources. Gai et al. [20] explored privacy-preserving edge frameworks based on blockchain technology, thereby ensuring end-to-end data integrity over public and untrusted networks.

IV. COMPREHENSIVE LITERATURE EVALUATION MATRIX

This section offers a clear, direct comparison of the key research papers selected for this review. comparing them together helps reveal major design trade-offs, trace how edge computing has grown, and highlight challenging issues researchers still cannot fully solve. Table 2 presents the corresponding evaluation matrix for comprehensive literature review.

Table 2: Literature Evaluation Matrix

Citation	Primary Edge Tier	Optimization Methodology	Primary Systemic Goal	Security Profile Provided	Target Use-Case / Constraints
Shi et al. [1]	Far Edge to Cloud	Conceptual / Reference Model	Architectural Viability	High-level Privacy Bounds	Generic Edge Computing Paradigm
Mouradian et al. [2]	Near Edge Gateway	Hierarchical Network Topology	Multi-tier Interoperability	Decentralized Node Integrity	Fog Orchestration Systems
Mach & Becvar [3]	Cloudlet (MEC)	Deterministic Offloading Policy	Offloading Latency Reduction	Baseline Radio Access Security	Telecommunication Networks
Lu et al. [4]	Multi-Tier Continuum	Collaborative Synchronization	System Response Realism	Trust Chain Verifiability	Industrial IoT / Digital Twins
Martinez et al. [5]	Far Edge	Embedded Local Processing	Data Traffic Filtration	Physical Hardware Hardening	Manufacturing Floor Sensors
Deng et al. [6]	Near Edge to Cloud	Deep Reinforcement Learning	Edge Intelligence Synergy	Local Data Isolation	Dynamic Mobile web Tasks
Aslanpour et al. [7]	Multi-Tier Continuum	Low-Overhead Heuristics	Fast Task Mapping Turnaround	None (Assumes Trusted System)	Heterogeneous Public Clouds
Rawat & Parwez [8]	Cloudlet (MEC)	Game Theory (Nash Markets)	Fair Resource Balancing	Anti-Monopolization Tracking	Shared Multi-User Environments
Dinh et al. [9]	Near Edge Gateway	Statistical ML Prediction	Congestion Pre-emption	Baseline Transport Layer Sec.	High-Velocity Traffic Streams

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IX Sep 2026- Available at www.ijraset.com

Zhou et al. [10]	Far Edge to Cloudlet	Federated Model Aggregation	Bandwidth + Privacy Co-Design	Gradient Anonymization	Decentralized Edge Inference
Zhang et al. [11]	Far Edge	Strict Scheduling Deadlines	Latency Minimization	Wireless Signal Privacy	Time-Critical Safe Operations
You & Huang [12]	Near Edge Gateway	Dynamic Offloading Balance	Energy Consumption Drop	Battery Drain Preservation	Portable / Battery Smart Nodes
Luan et al. [13]	Near Edge Gateway	Localized Cache Redundancy	Bandwidth Conservation	Inverted Hash Verification	High-Definition Video Feeds
Wang et al. [14]	Cloudlet Layer	Economic Provisioning Pricing	Infrastructure Operational Cost	Multi-Tenant Infrastructure Sec.	Commercial Micro-Cloud Rental
Shafique et al. [15]	Multi-Tier Continuum	Thermal-Aware Management	Green Carbon Reductions	Environmental Node Isolation	Large-Scale Decentralized webs
Xiao et al. [16]	Far Edge to Cloud	Multi-Tenant Surface Mapping	Security Threat Delineation	Complete Threat Spectrum	Vulnerability Auditing Systems
Al-Turjman [17]	Far Edge	Low-RAM Symmetric Primitives	Processing Cost Efficiency	Lightweight Device Encryption	Micro-Chip / IoT Deployments
Sun et al. [18]	Near Edge Gateway	Zero-Trust Framework Maps	Identity Trust Preservation	Mutual Authentication Chains	Dynamic Ad-Hoc Meshes
Khan et al. [19]	Cloudlet Layer	Hardware Cryptographic Anchor	Physical Tamper Resistance	Trusted Execution Isolation	Unattended Street-Side Stations
Gai et al. [20]	Multi-Tier Continuum	Ledger Consensus Validation	Multi-Channel Data Integrity	Blockchain Cryptographic Ledger	Open Distributed Public Channels

The comparison table shows key trends, the major trade-offs, and how edge computing is changing today. Taken as a whole, the research points to three main insights about building distributed systems:

1) The Latency-Energy Trade-Off: System designers have to keep trading speed for power use all the time [21]. Systems built for ultra-low latency usually need a constant network link and top-level processing, so the battery drains quickly. On the flip side, energy-focused designs may add small waiting time or pause tasks in local queues, helping battery-powered devices last longer.
2) The Rise of Adaptive Intelligence: People are moving away from fixed, static mathematical formulas and toward smarter, AI-powered solutions that adapt as needed. Early edge systems depended on strict rules, but they often failed when network conditions shifted. Modern studies use deep reinforcement learning with federated learning so edge devices can adjust on their own when traffic surges suddenly and wireless signal strength varies.
3) The Security Overhead Conflict: Implementing robust security in a distributed network introduces a major performance penalty. Advanced defensive measures, such as blockchain ledgers or hardware isolation, provide excellent protection against tampering. However, these methods require heavy computational work that frequently contradicts the low-power, resource-constrained goals of far-edge IoT devices.

V. OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

The architectural, algorithmic, and cryptographic frameworks discussed in this paper have revealed systemic vulnerabilities across the edge-cloud continuum. By examining the current state of the art, it's pertinent that extreme hardware variations are still hampering the progress of edge computing paradigm. Low-power edge devices do not get the consistent software tools they need to communicate smoothly with stronger cloudlets or multi-level networks. Because of edge nodes mobility, the network becomes volatile, and tasks often halt mid-execution. Some current frameworks use quick, low-cost heuristics to schedule tasks, but these models depend on fixed assumptions that fail when nodes suddenly disconnect. Far-edge hardware has strict resource limitations, which makes this problem even worse.

When developers try to add zero-trust authentication and protect data integrity on these networks, the cryptographic processing becomes too heavy, overwhelms the small batteries and processing power of the local nodes. At last, most optimization work only tries to cut raw delay or keep each node's battery from draining, but researchers still largely ignore how heat builds up across the system and how to schedule tasks with carbon-aware parameters in mind for distributed micro-clouds.

To fix these architecture problems, future research should shift away from relying on isolated local fixes and instead use cohesive, multi-layered solutions. Instead of relying on separate, vendor-only gateways, new systems should use lightweight, open-source middleware and common API designs that let resources move smoothly across layers. Second, to prevent data loss when nodes move, task offloading systems should stop relying on fixed scheduling rules. New systems should blend reinforcement learning with mobility-prediction models, so devices can forecast where they will move and switch data connections to the next link before a physical drop happens. Third, engineers must tackle the security paradox by designing hardware and software jointly, so strong encryption can work on low-power devices. It means building special hardware security tools that run fast and fit neatly into the tiny space of new microcontrollers. To create lasting networks, carbon efficiency has to be treated as a main priority. This requires designing thermal-aware scheduling algorithms that tie the workload distribution directly to the availability of localized, renewable energy sources.

VI. CONCLUSION

This survey paper gives a clear, well-organized picture of edge computing by sorting today's research into a simple set of categories. The paper traces the technology's evolution, showing how it shifted from network layers and algorithms to system goals and security safeguards. The final part of the paper says edge computing has moved beyond old, fixed algorithmic models and now relies on smarter, more flexible AI solutions. Engineers are stuck balancing two demands: quicker networks drain the battery, while security work needs lots of computing, so the system has to manage speed, power use, and safety together. To make edge computing run smoothly in real life, it needs to handle hardware standards, keep moving devices working, cover security costs, and still power everything with greener energy.

REFERENCES

[1] W. Shi et al., "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, Oct. 2016.
[2] C. Mouradian et al., "A Survey on Fog Computing: Architecture, Key Technologies, and Open Issues," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1716–1740, 3rd Quart. 2018.
[3] P. Mach et al., "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1628–1656, 3rd Quart. 2017.
[4] Y. Lu et al., "Communication-Efficient Federated Learning and Digital Twins for Intelligent Device-Edge-Cloud Cooperative Computing," IEEE Internet of Things Journal, vol. 8, no. 23, pp. 17212–17225, Dec. 2021.
[5] J. Martinez et al., "Far-Edge Computing for Industrial IoT: Architecture and Performance Evaluation," IEEE Transactions on Industrial Informatics, vol. 17, no. 9, pp. 6331–6341, Sep. 2021.
[6] S. Deng et al., "Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7457–7469, Aug. 2020.
[7] M. S. Aslanpour et al., "A Heuristic Task Scheduling Algorithm for Heterogeneous Edge-Cloud Systems," Journal of Systems Architecture, vol. 113, p. 101897, Feb. 2021.
[8] D. B. Rawat et al., "Game-Theoretic Optimization for Shared Resource Allocation in Mobile Edge Computing Networks," IEEE Transactions on Mobile Computing, vol. 21, no. 4, pp. 1212–1223, Apr. 2022.
[9] T. Q. Dinh et al., "Offloading Optimization for Mobile Edge Computing with Machine Learning-Based Workload Prediction," IEEE Transactions on Wireless Communications, vol. 19, no. 2, pp. 1279–1293, Feb. 2020.
[10] Z. Zhou et al., "Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing," Proceedings of the IEEE, vol. 107, no. 8, pp. 1738–1762, Aug. 2019.
[11] J. Zhang et al., "Energy-Receiver Relationship and Latency Optimization in Wireless Powered Edge Computing Networks," IEEE Transactions on Mobile Computing, vol. 20, no. 3, pp. 1095–1110, Mar. 2021.
[12] C. You et al., "Energy-Efficient Computation Offloading for Mobile Edge Computing," IEEE Transactions on Communications, vol. 22, no. 2, pp. 884–897, Feb. 2020.
[13] T. H. Luan et al., "Bandwidth-Aware Data Compression and Allocation Strategies at the Network Edge," IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4321–4334, Apr. 2020.
[14] X. Wang et al., "Cost-Effective Micro-Cloud Provisioning for Edge Computing Infrastructures," IEEE Systems Journal, vol. 15, no. 2, pp. 2102–2113, Jun. 2021.
[15] M. Shafique et al., "Green Edge Computing: Challenges, Solutions, and Future Directions," IEEE Access, vol. 9, pp. 128901–128918, Sep. 2021.
[16] Y. Xiao et al., "Security and Privacy in Edge Computing: A Contemporary Survey," IEEE Micro, vol. 40, no. 1, pp. 10–22, Jan.–Feb. 2020.
[17] F. Al-Turjman et al., "Lightweight Cryptographic Protocols for Securing Resource-Constrained Edge Devices," IEEE Communications Magazine, vol. 57, no. 10, pp. 88–94, Oct. 2019.

[18] X. Sun et al., "Authentication and Access Control Frameworks in Distributed Edge Networks," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 4, pp. 1822–1836, Jul.–Aug. 2021.
[19] A Khan et al., "Physical Tamper-Resistance and Hardware Security for Scattered Edge Nodes," IEEE Systems Journal, vol. 16, no. 1, pp. 542–553, Mar. 2022.
[20] K. Gai et al., "Privacy-Preserving Edge Computing via Blockchain and Federated Learning Mechanisms," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11899–11911, Jul. 2022.
[21] Mohammad S. A. et al., "Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research", Internet of Things, Volume 12, 2020.
[22] Kashif Bilal et al., "Potentials, Trends, and Prospects in Edge Technologies: Fog, Cloudlet, Mobile Edge, and Micro Data Centers", Computer Networks, 2017.
[23] Kurt Geihs et al., "Performance Analysis of Edge-Fog-Cloud Architectures in the Internet of Things", IEEE/ACM 13th International Conference on Utility and Cloud Computing, pp 374-379, 2020.
[24] Jain Arpit et al., "An edge computing paradigm for time sensitive applications", Fourth World Conference on Smart Trends in Systems, Security and Sustainability, pp 798-803, 2020.
[25] Karim Faria et al.,"To edge or not to edge?", Symposium on Cloud Computing, pp 629, 2017.
[26] Naveen Soumyalatha et al., "Key technologies and challenges in IOT edge computing", Third International Conference on I-SMAC, pp 61-65, 2019.
[27] Shi et al., "Edge Computing: Vision and Challenges", IEEE Internet Of Things Journal, Vol. 3, No. 5, pp 637-646, 2016.
[28] Uddin Mohammed et al.," A Review on Edge to Cloud: Paradigm Shift from Large Data Centers to Small Centers of Data Everywhere", Fifth International Conference on Inventive Computation Technologies, pp 318-322, 2020.
[29] B. Varghese et al., "A Survey on Edge Performance Benchmarking", ACM Computing Surveys, Vol. 54, No. 3, Article 66, 2021.
[30] Yousefpour Ashkan et al., "All one needs to know about fog computing and related edge computing paradigms: A complete survey", Journal of Systems Architecture, pp 289–330, 2019.