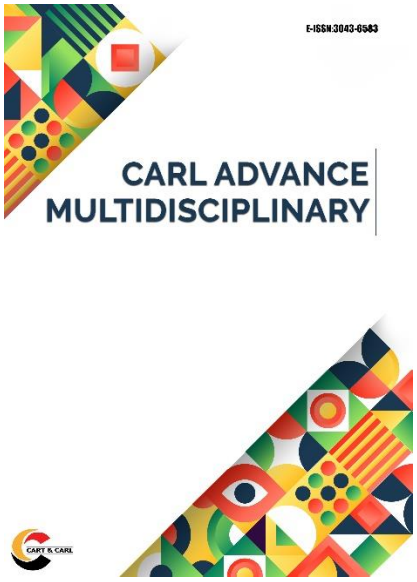
Review

CARL ADVANCE MULTIDISCIPLINARY
https://cartcarl.com/journal/carl-advance-multidisciplinary

E-ISSN: 3043-6583




# Edge Computing Architecture within the Application Area of Internet of Things (IoT) Devices: A Review

**Authors**
[a] Alabi, A.O., [a]Onungwe, H.O.

[a] Department of Computer science, Faculty of Computing, University of Port Harcourt, Port Harcourt, Nigeria.

**Corresponding Author**
Alabi, A.O.
(akinity2000@yahoo.com)

Received: 05 January 2025
Accepted: 15 February 2025
Published: 12 March 2025

**Citation**
Akintomide, A.O., Onungwe, H.O. (2025). Edge Computing Architecture within the Application Area of Internet of Things (IoT) Devices: A Review. *Carl Advance Multidisciplinary*, 2(1), 9-13. https://doi.org/10.70726/cam.2025.210913

## Abstract

The spread of Internet of Things (IoT) devices has led to an exponential increase in data generation, transmission, and processing. However, the traditional cloud-centric approach to IoT data processing has several limitations, including high potential, bandwidth limitations, and security worries. Edge computing has emerged as a capable solution to address these challenges by processing data closer to the source, i.e., at the edge of the network. This paper presents an all-inclusive review of edge computing architecture within the application area of IoT devices. We discussed the key components, architectures, and technologies that enable edge computing, including fog computing, mist computing, and cloudlet. We also explore the benefits and challenges of edge computing in IoT applications, such as real-time processing, reduced latency, improved security, and increased scalability. Furthermore, we identify the research gaps and future directions in edge computing for IoT devices, including the need for homogeneous architectures, efficient resource management, and robust security devices.

Keywords : Edge Computing, IoT Devices, Fog Computing, Mist Computing, Cloudlet, Scalability

## Introduction

The Internet of Things (IoT) has revolutionized the way we live and work, with billions of devices connected to the internet, generating large amounts of data [1, 2]. However, the traditional cloud-centric approach to IoT data processing has several restrictions, including high potential, bandwidth constraints, and security worries [3,4]. To address these challenges, edge computing has emerged as a helpful solution, enabling data processing closer to the source, i.e., at the edge of the network [5,6]. Edge computing is a distributed computing paradigm that brings computation closer to the source of the data, reducing latency, improving real-time processing, and enhancing security [3,4]. In the context of IoT devices, edge computing enables data processing and analysis at the edge of the network, reducing the need for data transmission to the cloud or centralized data centers [7,8]. The application of edge computing in IoT devices has numerous benefits, including improved real-time processing, reduced latency, enhanced security, and increased scalability [3.4]. However, edge computing also poses several challenges, such as managing and orchestrating edge resources, ensuring security and privacy, and addressing the complexity of edge computing architectures [7,8].

Edge Computing is the strategy of handling information at the nearby areas rather than a cloud information handling stage where information

is produced. Rather than being moved to a server farm, information is handled by the actual device or by a neighborhood PC or server in edge processing. Current businesses have been embracing edge Computing with numerous potential applications. Edge computing has been around for some time now and producers are investing a lot of energy into advanced change, otherwise called Industry 4.0 since they should be more adaptable and savvy in dealing with their offices and tension on their center business inferable from worldwide contest. Portable and IoT applications are the critical drivers of edge security and processing. Industry 4.0 also known as the Smart Manufacturing is the 4th evolution of industrial technology that uses embedded systems and other smart technologies to connect with other devices in order to manufacture tangible products for users need. Although, its scope is much wider than smart machines. The quantity of versatile and IoT applications is quickly expanding. Edge Computing additionally incorporates 5G innovation [9].

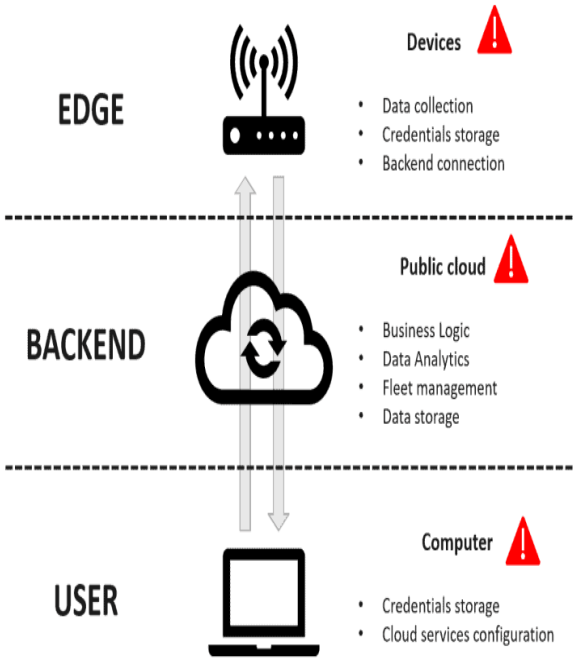



Figure 1: Edge Computing in Public Cloud

**Security Concerns in Edge Computing**

Since Edge devices processes critical data, low knowledge of the use of these devices can cause violation of privacy. Edge devices are components that are used in processing data in a local format ere it is sent to a server, e.g. smart cameras, robotics controllers, wearable devices, drones etc. Some concerns in Edge Computing are:

*Hardware Backdoors*: When manufacturers uses cut and nail processes, it can lead to unseen vulnerabilities in Edge devices.

*Malicious Attack*: Black Hat Hackers can manipulate data items by making a device to read false information, thereby creating data inconsistencies which may lead to forcing the systems to make incorrect decisions and reports.

*IOT Ecosystem*: IOT is made up of a wide range of networks and applications connectivity. Each of these connectivity has its own peculiar vulnerability, talk more of when there are more of these vulnerabilities in a singular Edge device, it creates a colony of vulnerable challenges.

**Characteristic of Edge Computing**

*a. Problem Identification*

Current ventures are reviving with IoT applications that can be applied in smart homes, building computerization frameworks, transportation frameworks, smart Cameras, etc. IoT, and different devices associated with the edge to accumulate, make, and interaction information, all conceivably prior to managing a regular security machine, edge Computing is on course to become one of the most intensely visited places of an industry. Selvaraj et. al. [10] and Xiao et. al. [11] showed that it is possible to control the IoT tangible device from the actual layer by a hacker, by identifying mocking assaults in remote organizations, Liao et. al. [12] investigates actual layer validation and works on the security of the versatile edge processing (MEC) framework. Quick advancement of edge processing expands the security weaknesses. The fifth era (5G) network fabricate utilizing innovation of Virtualized Multi-access Edge Computing (vMEC), Software Defined Networking (SDN) which upholds numerous IoT device [8]. A survey [6] in IoT application showed that IoT applications might put the actual frameworks in danger. By conveying counterfeit ARP messages through the edge organization, aggressors parody Media Access Control (MAC) locations and connection them to the IP locations of true edge devices utilizing Address Resolution Protocol (ARP) [13].

b. Industrial and IoT applications: processes highly sensitive industrial data items, locally in order to reduce vulnerability to cyber attacks
c. AI and Machine Learning at the Edge: AI-based edge sensors are used to detect grid failures and voltage drops on cyber attacks
d. Real Time Processing: Real-Time Decision making is done to reduce response time for complex problems. These analytics also reduces waste and improve efficiency precision at smart cities.

**Challenges on Developing Technologies**

Data transmission is one of the vital components of fostering an edge computing device [13]. Some of the challenges on developing technologies are:

Programmability: is a challenge in edge computing because the various range of edge devices, with different hardware capabilities and operating systems, often require different programming languages and frameworks, making it difficult to develop a single, unified codebase that can run across all edge nodes, which eventually leads to complexity in development, management, and maintenance.

Naming – Naming is a way of uniquely identifying devices, data and services across a distributed network. Edge Computing involves billions of interconnected devices, as such, it makes it difficult to assign names to these wide range of connections. For instance, if two IoT sensors in a particular area are given same name, it can lead to conflicts and misrouting of data during analysis. Naming instrument of edge hubs are extremely mind boggling because of immensely enormous types of IoT devices.

Data Abstraction – Data Abstraction is executed by displaying only the vital information and abstracting (hiding) the less important information of a dataset. In Edge Computing, data is processed at different levels/layers of IoT devices, if Abstraction is not properly managed for data flow across these layers, it creates inconsistencies and possible loss of data. This is becoming more testing in light of colossal number of information generators can be put in single IoT device [14]. The ascent of edge processing has led to new online protection concerns. The present online protection endeavors center fundamentally around the endpoint and organization, leaving the edge more presented to assault [15].

**Edge Computing Architecture**

In recent years, giant strides have been made in promoting the Edge Computing architecture, yet there is a need for more improvement. Currently some of Edge Computing efforts appear to be in specific applications, software stacks, sources of data being used, specific cloud and network service providers. This various fragmentation across different service providers and multitude of software stacks constrain the stakeholders from realizing the full potential of Edge Computing. There is a need for a proper amalgamation of these diverse domains through standardization, industry alliances and market forces[16].

**Application Area of IoT Devices**

The underlisted are the application areas of IoT devices in Edge Computing:

a. Robotics: use IoT devices to connect robots that can interact with humans and terh machines at the edge in order to enhance productivity and safety.

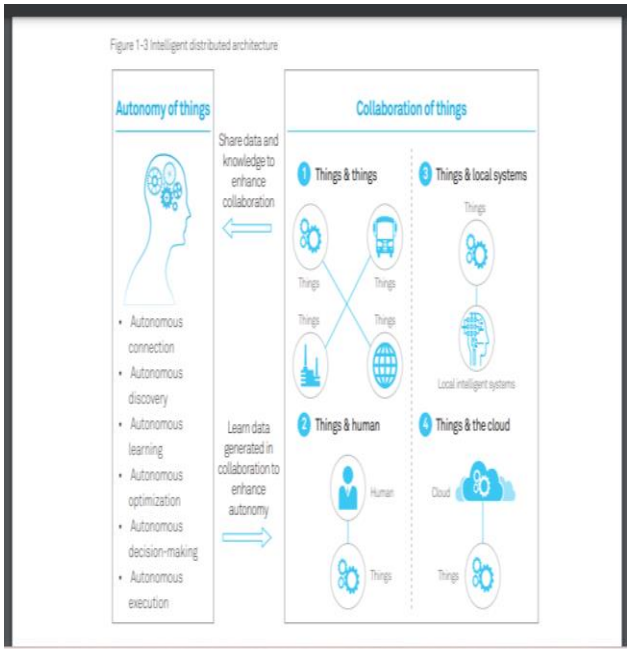


Figure 2: Edge Computing Architecture

b. Disaster Monitoring: uses IoT Wildfire devices placed in a forest to detect and monitor smoke, temperature and humidity in order to provide warnings
c. Smart Grids: Avoid overloads by using Edge nodes to manage and optimize energy load distribution across grids and equally use IoT devices to monitor solar panels and batteries, etc.
d. Livestock Monitoring: using wearable IoT devices on animals to monitor statistics. IoT censors can also be used to monitor crop health.

**Literatures Review**

With regards to edge computing, transmission inertness [17] and battery-arranged energy [18] , transmission inactivity is a central issue for IoT device which prompts information anomaly and it additionally summarizes that low fuelled devices can make high dormancy transmission [19]. Zhao et al. [1] and Wang et al. [3] additionally investigated actual layer security, which is anticipated to exploit the current actual layer security approaches' similarity and consistency.

**Future Work**

In Edge Computing, security and protection prerequisites, security and security dangers, and the scientific categorization of assaults influencing the edge network are talked about [9]. It infers that more examination in this field of study can foster a superior arrangement, as the reconciliation of Industry 4.0. advancements for the improvement of "brilliant urban communities" is developing, and shrewd use of this innovation is relied upon to expand consumption.

## Conclusion

Edge computing is a half breed of cloud and local computing. The cloud is used to ship and store data services.. Edge Computing, when combined with IoT devices is used to show how data is processed by bringing data processing very close to the source of data generation which is the IoT device itself. Whereas, it is used for real time precise decision making, however, it carries inherent vulnerabilities of different layers of devices posing a lot of security concerns, which if not addressed, will lead to data inconsistencies and outright loss of vital information. Edge Computing with IoT devices enables faster, smarter and more reliable systems.

The strategy for edge computing is generally utilized in home mechanization, shrewd urban communities, and other IoT frameworks. As the Internet of Things (IoT) business develops, hackers will actually want to oversee a vulnerable framework, representing a significant threat and trust issue for end-user-clients. Besides, an attack could affect the presentation of IoT devices.

## Declaration of Competing Interest

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.

## Credit Authorship Contribution Statement

All authors contributed equally.

## References


1. Zhao, X. Zhang, J. Chen, and L. Zhou, "Physical Layer Security in the Age of Artificial Intelligence and Edge Computing," IEEE Wireless Commun., vol. 27, no. 5, pp. 174–180, Oct. 2020, doi: 10.1109/MWC.001.2000044
2. R.-F. Liao et al., "Security Enhancement for Mobile Edge Computing Through Physical Layer Authentication," IEEE Access, vol. 7, pp. 116390–116401, 2019, doi: 10.1109/ACCESS.2019.2934122.
3. D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City," IEEE Access, vol. 7, pp. 54508–54521, 2019, doi: 10.1109/ACCESS.2019.2913438.

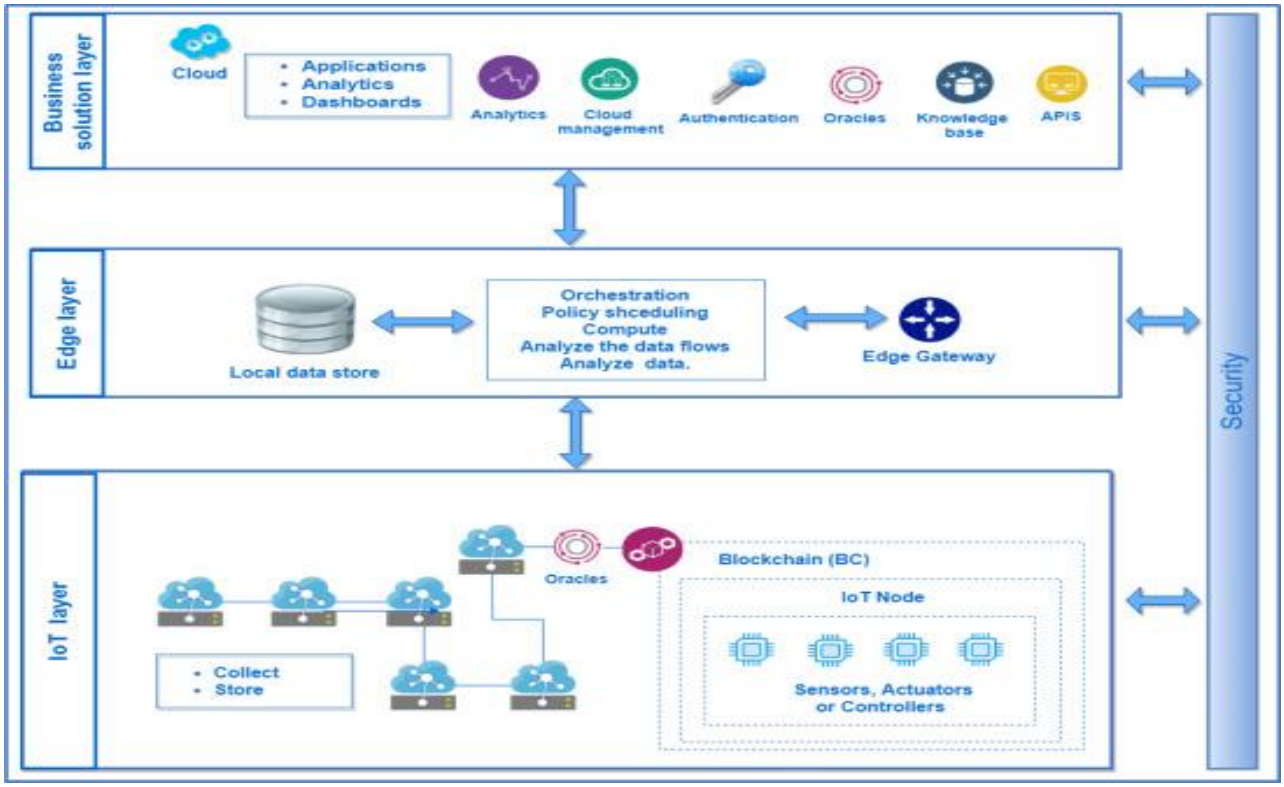




Figure 3: "Future Generation Computer Systems," [14]

4. S. Trinks and C. Felden, "Edge Computing architecture to support Real Time Analytic applications : A State-of-the-art within the application area of Smart Factory and Industry 4.0," in 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, Dec. 2018, pp. 2930–2939. doi: 10.1109/BigData.2018.8622649.
5. "Five edge computing use cases for the manufacturing industry," STL Partners. https://stlpartners.com/edge_computing/five-edge-computing-use-cases-manufacturing-industry/ (accessed Oct. 01, 2021).
6. K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," Digital Communications and Networks, vol. 6, no. 2, pp. 195–202, May 2020, doi: 10.1016/j.dcan.2019.08.006.
7. F. O. on March 2 and 2021, "Edge Computing Growth Drives New Cybersecurity Concerns," Security Boulevard, Mar. 02, 2021. https://securityboulevard.com/2021/03/edge-computing-growth-drives-new-cybersecurity-concerns/ (accessed Oct. 01, 2021).
8. Umamaheswar (Achari) Kakinada, Deh-Min Richard Wu, Curt Wong and Yildirim Sahin: "Edge Computing Architecture (2021)" – Fall Technical Forum – Virtual Experience, SCTE CableLabs and NCTA.
9. H.-C. Hsieh, J.-L. Chen, and A. Benslimane, "5G Virtualized Multi-access Edge Computing Platform for IoT Applications," Journal of Network and Computer Applications, vol. 115, pp. 94–102, Aug. 2018, doi: 10.1016/j.jnca.2018.05.001.
10. M. Yahuza et al., "Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities," IEEE Access, vol. 8, pp. 76541–76567, 2020, doi: 10.1109/ACCESS.2020.2989456.
11. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198
12. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198
13. Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge Computing Security: State of the Art and Challenges," Proc. IEEE, vol. 107, no. 8, pp. 1608–1631, Aug. 2019, doi: 10.1109/JPROC.2019.2918437.
14. J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic Induction Attacks Against Embedded Systems," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security, Incheon Republic of Korea, May 2018, pp. 499–510. doi: 10.1145/3196494.3196556.
15. A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, "Artificial Intelligence-Driven Mechanism for Edge Computing-Based Industrial Applications," IEEE Trans. Ind. Inf., vol. 15, no. 7, pp. 4235–4243, Jul. 2019, doi: 10.1109/TII.2019.2902878.
16. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.
17. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.
18. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.
19. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.