e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

EDGE COMPUTING IN IOT: A COMPARATIVE REVIEW

Shobhit Singh*1, Dr. Anil Kumar Pandey*2

*1,2Department Of Computer Science & Engineering, Shriramswaroop Memorial University,
Barabanki, Lko, India.

DOI : https://www.doi.org/10.56726/IRJMETS71936

ABSTRACT

Edge computing has gradually availed itself as one of the most important technologies in the Internet of Things (IoT) to influence the processing, management, and utilization of data. A major advantage that is offered by edge computing by bringing computation and storage resources closer to IoT devices is that it minimizes latency as well as conserves bandwidth and offers greater capabilities for real time decision making. These changes from massive cloud processing to multiple neighboring edge nodes solve IoT architectural challenges common in earlier types of design, including those with low-latency responses and offline capabilities of applications such as smart cities, self-driving cars, and industrial control systems. The potential advantages of edge computing in IoT include privacy and security, because the collected information can be analyzed on the fly on the endpoint without sending it to the cloud; scalability, given that a great amount of IoT devices can be monitored by edge nodes without putting extra load on the centralized facilities. However, the use of edge computing in IoT also poses some challenges for example restricted resources at edge nodes, issue of the network infrastructure and more so the security that has to be enhanced. This abstract discusses the existing works done on architecture of edge computing IoT, the advantages and the limitation of integrating edge computing IoT system and indicates how it is capable of revolutionizing industries and enable a new IoT generation application system equipped with intelligence and decentralization.

I. INTRODUCTION

As the new technology accelerates at a relentless pace, the IoT is a new way modern people experience the environment. IoT can thus be described as a system of linked devices that are capable of gathering, transmitting as well as processing data. These devices run the gamut from just basic sensors and consumer wearables to complicated industrial equipment and management systems in smart cities. Statistically, the number of IoT devices is projected to exceed 30 billion by 2024, and each of these devices will be creating big data in terms of bytes per second. This creation of smart devices has led to numerous developments helping various sectors such as healthcare, agriculture, production, transportation, and the likes. However, this brings about a set of fundamental concerns that the conventional cloud computing models cannot effectively solve such as data processing delay, traffic jam, data insecurity, and expansion complications.

Most of IoT frameworks employ the cloud architecture for aggregation, processing, and storage of information right from the commencement of the internet of things. In this model, the data generated by the IoT components is sent to the internet and stored in a cloud-based system that processes as well as analyzes the information and sends it back either to the devices or the consumers of the information. Nevertheless, this method has all grounded many led to the design and implementation of many different IoT tools.

Today such architecture reveals several drawbacks which are getting expanded due to the larger size and complexity of IoT networks. This is because, with a growing number of IoT devices comes a tsunami of data that these devices generate. Sometimes it may be too much for network sources resulting to a delay in delivering messages or an increase in latency which is, the time taken by information from the source to the intended destination point or point back to the starting point again. High latencies are especially critical for real-time applications such as autonomous cars, remote health monitoring, automation control in industries, and the control systems of electrical grids located in various regions where even a few milliseconds of difference could be crucial in making the right decision.

The reason being, with the increasing number of IoT devices comes an avalanche of data that they produce. At times this influx can be too much for network sources leading to delays in sending messages or increase in latency which is time taken by information from source to destination point or point back to its starting point again. Very high latencies are particularly significant for real-time applications e.g. autonomous automobiles, remote medical observations, automation managements within industries as well as control systems within electric grids distributed throughout different areas where even a few milliseconds can mean a decision-making difference between success and failure.

Moreover, centralized cloud computing poses significant security and privacy issue since they are centralized. When the recorded data is sent through large distances to centralized servers, such information is at risk of attacks like data breaches, interception among others. The risks are particularly high in IoT context since many connected devices are not powerful enough to perform a necessary level of security protection. Also, some IoT use cases entail handling even user data, which for certain applications such as healthcare and financial services, need to have very high privacy consideration. Storing such data in the central cloud storage platform may have a serious issue of privacy since the data may be exposed to threats in transit and storage.

II. LITERATURE REVIEW

Edge computing has been acknowledged as an emerging solution in facilitating shifts within the IoT environment while contrasting with the centralized cloud adaptation. This literature review seeks to identify how these aspects are addressed in the literature with regards to edge computing in IoT concerning architectural models, performance enhancements, security and privacy, resource management, AI accommodation, and heterogeneity and scalability challenges. This review also shows the real-world applications of edge computing in various domains to discuss its implications in practice as well as potential areas of future research.

1. Here we first discuss the architectural models of edge computing in IoT.

1.1 Introduction: The Concept of IoT Along with its Conventional Architecture

Based on the literature review, the initial architectures of IoT applied a conventional cloud model to address the storage, computation, and analysis tasks. It is known that IoT devices (sensors, actuators, etc.) of the terminal collect data on objects, and transfer it to the computation and decision-making center in the cloud servers. This model is suitable for application scenarios where the system is not required to respond immediately but there are disadvantages which include high latency, high bandwidth consumption and the inability to keep data private at the same time. Shi et al. also pointed out in their study that there are four major disadvantages of the cloud-centric model, which is high latency, high bandwidth consumption, security vulnerability and thus not suitable for time-sensitive and mission critical applications

1.2 Edge Computing Architecture for the Internet of Things

This, however, is where edge computing comes in as it changes a paradigm by performing computations nearer to the data than in traditional cloud computing. Key architectural models include:

Fog Computing: According to Bonomi et al. (2012), fog computing takes cloud services to the network fringes, intermediated by the 'fog nodes' between IoT devices and cloud servers. Fog nodes which are furnished at the local gateways or routers, provides computing, storage and networking. This architecture is effective as it is able to lower the latency and bandwidth requirement as well as improving on data security by storing data locally or at a regional level.

Cloudlets: Other researchers such as Satyanarayanan et al. (2009) proposed a new architecture which includes what they call cloudlets, which are basically small-scale data centers close to IoT devices. Cloudlets afford local computing proximity with low latency and high processing for imperative use cases including augmented reality and video analytics. In this way, the evaluated approach presents the primary advantage of the cloudlets for offloading complicated computations from IoT devices while achieving fast response times.

Micro Data Centers: Srirama et al. (2017) presented micro data centers which are relatively miniature versions of conventional data centers, specially located in the network peripheries. These centers cater for localized data processing and storage and therefore minimize the distances that data has to travel to reach central clouds. Micro data center can be applied to IoT environment with massive data transmission including smart city and industrial applications. These architectural models represent the framework for deploying the edge computing in IoT so that it can strike a middle ground between centralized and distributed computing.

2. Performance Optimizations via Edge Computing

2.1– Lower Latency and Real Time operation

This is one of the most important advantages of edge computing in IoT in which the latency is reduced substantially. For data processing it was further evidenced in Wang et al. (2018) that edge computing reduces data transmission time through data processing at the edge. In such scenarios like self-driving cars, real-time decisions should be made within microseconds and with edge computing this is made possible. For example, edge- based V2X communication systems enable real-time analysis of data collected by sensors and cameras and act as real-time traffic monitoring systems having information on possible dangers or the best routes to take.

2.2 Bandwidth Management and Minimization of Costs-

Edge computing thus minimizes data sent to cloud as data is filtered, aggregated, and analyzed at edge. As stated by Zhang et al. (2020), this local processing brings down the amount of bandwidth usage and expenses linked with data transfer and data storage in the cloud. In smart city applications for instance, edge nodes can aggregate and analyze data from thousands of sensors measuring air quality, traffic flows, and energy consumption; forwarding on only Significant data to the cloud for further processing. It also helps in conserving the bandwidth, minimize operational expenses and guarantee delivery of data within the required time.

2.3 Better reliability and availability

Edge computing also makes IoT systems more reliable and available since the processing of data occurs on different edge nodes. Other authors, such as Abouaomar et al. (2019), described that edge computing offers resiliency since IoT devices can run independently of the cloud link. In industrial IoT context, edge nodes can control local processes, diagnostics and remedial actions without requiring support from distant cloud servers, as for continuous operational readiness.

Security and Privacy in Edge Computing for IoT

1. Security Issues in Conventional Cloud-Based IoT Architectures

Current cloud-based IoT systems are prone to one or a combination of data breach, interception, or unauthorized access. Information being exchanged between different IoT devices and the cloud is vulnerable to possible attackers, and the centralized 'cloud' is a weakness with all data in a specific location. In their paper, Yang et al. (2017) mentioned that the increased amount of data transferred and stored in centralized clouds enhances the potential of the attack vectors and hence C/IoT models are at a higher risk of cyber threats.

2. Increasing Security Through Edge Computing

Dealing with data at the edge can alleviate some security challenges since fewer sensitive data interacts with external networks that may be less secure. Kandukuri et al. (2018) mentioned that edge devices can also enforce security locally at the source site by incorporating techniques like encryption, secure access control, and intrusion detection to ensure the data's safety. For instance, in healthcare systems, patient information can be analyzed at the edge to prevent information leaks as data is processed at the edge instead of being transferred to a cloud server.

3. Privacy Preservation Techniques at the Edge

Privacy preservation is critical in the use cases like health care and smart homes where patients' information should not be exposed to other parties. As described by Sun et al. (2019), there are three categories of privacy-preserving architecture for edge computing which include; Homomorphic Encryption, Differential privacy, Secure Multiparty Computation. These techniques make it possible to continue carrying out data analysis locally with the privacy of data maintained and this is an effective solution on how the data can be protected while at the same time the analysis can also be done.

4. Resource Management and Control for Reference Computing

4.1 Characteristics of Good Resource Management

Resource management in edge computing focuses on how the computing, storage as well as communicate resources are employed in order to yield the best outcome. These resource management related approaches that were presented by Liu et al. (2021) includes load sharing, task shifting, and dynamic resource for edges computing resources. In IoT settings, edge devices might not have large resource endowments hence the need to manage the limited resources in a way that will offer the desired performance.

4.2 Task Offloading Techniques

Task offloading as mentioned before is a process of transferring the computational tasks from IoT end devices to other nodes that possess higher processing capabilities at the edge or in the cloud. Masters et al (2019) enumerated some of the tasks offloading schemes; partial offloading where only several tasks are offloaded and opportunistic offloading where available resources are utilized. They improve the global behaviors of IoT systems through decreasing the usage of resources, including power consumption.

4.3 Energy efficiency is one of the major emerging trends of Edge-IoT environments. Power-usage is one of the core challenges for wirelessly powered edge-IoT devices that are often deployed in remote areas and likely to have batteries. Kim et al. (2022) explained various energy efficient computing algorithms and hardware platforms that helped in reducing overhead power consumption of edge devices while maintaining optimal flow. Methods like dynamic voltage scaling, energy-conscious task scheduling, and lightweight protocol enables edge applications to use energy efficiently and therefore sustain the devices used particularly in resource-scarce environments.

5. Intelligent Edge or Artificial Intelligence and Machine Learning Edge

5.1 Exploring the Possibility of Implementing AI and Edge Computing

Bringing AI and ML on the edge is crucial for IoT systems as it permits intelligent decisions in real-time without having to spend much time connected with the cloud. Accordingly, Zhang et al. (2019) stated that to minimize latency, edge AI models can analyses the data locally and find patterns of behaviors accordingly, for a prediction. This integration is very useful in such application areas such as predictive maintenance where failure in machines could be detected before time hence avoiding costly downtime.

5.2 OFF-LOAD Models for Intelligence at the Edge

AI models active at the edge are subjected to limitations of processing power and memory of the end devices. Chen et al. (2021) make use of methods such as model compression, pruning, quantization, and federated learning to design artificial intelligence models that can be deployed in the edge devices. These techniques help in keeping computational and memory requirement of AI models low to cater the edge devices, though their accuracy is not compromised.

5.3 Real-world Application of Artificial Intelligence at the Edge.

AI deployed at the edge has been proven useful in many areas including smart city, health care, and manufacturing. For instance, in smart cities, the edge AI is capable of processing real-time video stream from surveillance cameras to detect traffic violations, safety of the people and crowd management (Wang et al., 2020). In healthcare, edge AI refers to the use of data from the remote monitoring of patients through wearable gadgets where the data is analyzed to identify if there is any deviation and if there is an alert should be made to the health practitioners immediately (Li et al., 2022). Three major issues of concern are scalability and interoperability of multimodal interfaces, and the general availability of contextual information.

6.1 The Issue of Scalability in Edge IoT Networks

Another limitation found in edge computing is the scalability problem that majorly affects IoT networks involving numerous thousands or millions of edges. Han et al. (2020) pointed out that the handling of large traffic data, multiple data processing loads, and a plethora of resources in multiple edge nodes warrants systems for orchestration and coordination. The biggest challenge that comes with an ability to scale is the ability to do so without compromising on the speed, stability, and security of the services being offered.

6.2 Interoperability Challenges in Context of Heterogeneous Edge-IoT Settings Another important concern is the issues related to the connection between the edge and the IoT applications wherein many devices, platforms, and comm protocols are involved. Li et al. (2020) also talked about the fact that the absence of standardized edge computing frameworks can become a problem for proper integration of the corresponding components. Li et al (2020) also noted that such complexity and flexibility can lead to the absence of well-defined interfaces within the frameworks for different components, and

hence make interoperability between the IoT devices, the edge nodes and the cloud services difficult. That heterogeneity in turn can present problems in compatibility, for instance in setting up security protocols, data exchange format or modes of communication throughout the network architecture. In addition, the evolution of various types of devices and their operating systems increases the challenges of edge applications' implementation since every type of device is different and requires integration with different systems. In this regard, various interoperability frameworks and middleware solutions as postulated by researchers have been put forward. For instance, Broggi et al. (2021) proposed the application of open standards and the Interoperability protocols like the Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) for interconnecting of various IoT and edge devices. Secondly, middleware platforms which can offer layers of abstraction can facilitate the various hardware and software platforms to boil down to the common denominator, thereby facilitating system integration and management of the systems. These solutions have the objectives of simplifying the adoption of edge computing, especially in various IoT environments to increase scalability, flexibility and reusability.

7. Some of the real-life applications of edge computing in IoT are presented in the next subtopics.

7.1 Smart Cities

Smart city undertakings have incorporated the use of edge computing to address issues to do with, large sensor networks, traffic flow and transport optimization, safety measures, and environmental monitoring. For instance, when edge nodes are deployed at traffic lights and the nodes can perform video analytics on the feeds captured in real-time to determine congestion, accidents, or violation, then traffic management will be enhanced and responsiveness will be enhanced (Zanella et al., 2014). In the same way, air quality sensors that have edge computing can perform data analysis on the pollutant right on the spot so that city authorities can take immediate actions like warning the public or controlling traffic.

7.2 Industrial Automation

Decision-making: It would be crucial to make decisions on the fly in industrial settings and preferably on the edge of the computation; predict and prevent maintenance: One of the prominent use cases in industry 4. 0 application of edge computing; Real-time control of manufacturing processes; Safe operation in hostile environments. For instance, the devices deployed on production plant floor can monitor machines while distinguishing if an It has Issues or is experiencing some form of wear and tear, and alert for service before failure (Lee et. al. ,2018). This means that localized data processing reduces the amount of time spent, minimum spending on maintenance thus enhancing the efficiency of the used equipment. Similarly, complex automation and indispensable industrial robot control demand low latency and highly reliable communication; therefore, many new smart products support edge computations.

7.3 Healthcare

For this reason, edge computing is very relevant to the healthcare sector because it focuses on such applications as remote patient monitoring and telemedicine. Wearable and health smart accessories can capture a patient's data in real-time and hence it is possible to get an instant clue to the patient's health status (Rahmani et al., 2018). This capability is required for the type of events – very critical such as a case of heart attack or a fall – and help the care givers without the delay associated with cloud-based processing. Furthermore, edge computing assists in serving better protection of the data of the healthcare sector since that data is processed on the same edge, there and then to avoid the data's exposure to cybercriminals.

7.4 Autonomous Vehicles

Real Time data can only be processed in order to support self-driving cars, and for this purpose, the edge computing is crucial. Self-driving cars are equipped with many more sensors, cameras, and LIDARs to be able to comprehend the environment it is in, including how to navigate. By processing data at the edges, vehicles are in a position to detect cues such as nearby obstacles, and traffic signals and therefore can drive through complex areas with maximum delays (Molina-Masegosa & Gozalvez)., 2017). This ability to be safe and reliable in handling self-driving cars but especially in traffic must be localized

8. Future research directions

Some papers highlight the future capabilities and potential development of edge computing in IoT but there are some things that need deeper research to improve edge computing. First, future work should be directed towards increasing the scalability of the edge architecture across applications Second, some new research on how different interconnected systems can be integrated What third, explore security and privacy in the stream Fourth, explore AI and machine learning in a stream environment. Additionally, consistent proposals need to be developed to enable the integration of edge computing with new technologies such as 5G, blockchain, and quantum to create more complex and diverse IoT ecosystems.

III. METHODOLOGY

1. Data Collection

Primary Data Collection:

Interviews and Surveys: We also want to interview experts and professionals working in the IoT and edge computing fields, engineers and researchers. This data will provide an indication of how edge computing is viewed, the efficiency in practice, and some of the issues that are experienced when implemented.

Experimental Setup: Create a private setting in which IoT devices are programmed to feed data into edge nodes instead of a cloud center. This setup may involve using different type of devices such as sensors, camera, or gateway connected to edge nodes including Raspberry pie, Nvidia jetson or other industrial standard edge servers.

Secondary Data Collection:

Literature Review: Consult literature review and case studies which will reveal the state of knowledge on edge computing in IoT. These are areas that your research fills for lack of information and push towards their improvement.

Public Data Sets and Industry Reports: If supported by IoT datasets or reports, identify trends in latency or volume or cost when adopting edge computing.

2. Data Analysis Technique

Quantitative Analysis:

Latency and Response Time Measurement: Track and compare the latency between the edge computing and the cloud only models using Wireshark, or with a help of network simulator. Resource Utilization: Describe the usage rates and trends of CPU, memory, or bandwidth consumption for edge devices and then compare the use rates to what is observed in centralized systems in order to demonstrate the utilization efficiency enabled by Edge. Statistical Analysis: Use t-tests or regression analysis tests to determine whether latency, BW saving or/and speed differences are statistically significant.

Qualitative Analysis:

Content Analysis: Filter interview or survey data to find out more frequently mentioned aspects, for example, lower latency, better privacy, and faster data handling.

Thematic Analysis: In a similar way categories the qualitative primary data on the impressions of interviews & questionnaires about issues such as 'data privacy', 'network congestion', and 'costs' into 'benefits' and 'risks'.

3.Framework or Model Used Edge Computing Architecture: It discusses about the software structure that applied in the study, for example, the three level structure of device, edge and cloud layers, or a four-level structure of device, fog, edge and cloud (depending on the complexity of the model).

Custom Model: If a custom model or hybrid edge/cloud architecture was built, it should be understood (by the audience) what the layers are, what they do, and how they interact. Describe how the information moves through each layer and how it is analyzed.

4. Tools and Technologies

Hardware: Explain the type of edge devices that are incorporated as edge servers, edge gateways, or IoT edge sensors, and the features of the devices they possess, which consist of ppm, memory, or connection interfaces including 5G, Wi-Fi, Ethernet.

Software: It specifies the tools like edge computing frameworks, AWS Greengrass and Azure IoT Edge, and the processing libraries like TensorFlow Lite for edge AI, and networks like Monitor IoT.

Connectivity and Protocols: Explain how the objects of IoT connect to edge nodes using a network and undertake their communication through protocols like MQTT, CoAP, and WebSocket.

5. Performance Metrics

Latency: Calculate the parameters of changed end-to-end latency from the data generation stage till decision-making.

Bandwidth Savings: 215 Analyze data transfer rates for edge compute versus cloud only infrastructure.

Processing Speed and Load: Determine local compute rate and the evaluation of the edge devices CPU and memory usage during operations.

Energy Consumption: Quantitatively assess the energy usage of a given set of edge devices and compare it to, if possible, a centralized cloud computing platform.

6. Flaw of the Methodology

Scalability Limitations: It should also highlight any forms of limitations in scaling the edge network because of the restriction in hardware or energy.

Network Dependencies: Explain how networks availability and speed could affect the edges especially in a poor or unreliable network connection.

Generalizability: Indicate any limitations in the scope of its applicability because of a certain kind of devices or certain kind of network communicating over them.

IV. CONCLUSION

In addition to speed and security, the new edge computing shows significant advantages in the efficiency of network traffic usage and expenses. This means that organizations can be able to cut out the amount of data that they require to upload to the cloud hence cutting out the bandwidth as well as the costs tied to it. This advantage is especially valuable in scenarios where the communications connection is sporadic, or where data transmission fees are steep, as in remote industrial complexes, far-flung health facilities, and nomadic IoT operations. future research should build further on this study by constructively exploring the different scenarios for edge computing using different real-world settings and different types of networks.

Nevertheless, there still are several issues and drawbacks with the distribution of the IoT and the application of edge computing at present. Some of the limitations of this study include the fact that it does not address real world IoT networks fully, in as much as issues to do with network congestion, variability in the IoT devices' hardware and power constraints can influence performance. Future work can build upon these elements, investigate the costs of long-term operation, and investigate strategies for responding to challenges concerning hardware constraints, network robustness, and resource management at the edge.

Therefore, this paper concludes that edge computing is a promising line to develop future IoT systems. On the basis of their superior attributes involving low latency, secure and low-cost data processing it constitutes a key enabling technology for future IoT implementations. With growth IoT moving to every area of industry and society, edge computing will remain equally essential for creating efficient, secure, and sustainable IoT platforms as the need for real-time processing and data protection increases. This work presents important findings that go beyond identifying the current benefits of edge computing and outlines further developments that can fully unlock its potential and revolutionize various interconnected systems in many industries.

V. REFERENCES

[1] Zhang, Y., & Tao, F. (2020). Edge Computing: Next Generation IoT and IoE. Springer.

[2] Gubbi, Jayakanthan Buyya, Rita Marusic, Sanja Palaniswami, M. Internet of Things (IoT): A worldview, other aspects of design and potential future developments. Future Generation Computer Systems, 29(7), 1645-1660. https:>Accessed 16, October 2014 at
http://www.sciencedirect.com/science/article/pii/S016036091300204X
doi: 10.1016/j.future.2013.01.010

[3] 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. https: B. Ahmed, "An efficient routing privacy protocol for heterogeneous wireless sensor networks," Journal of Internet of Things, vol. 3, no.1, pp. 36–46, 2016, doi: 10.1109/JIOT.2016.2579198.

[4] Satyanarayanan, M. (2017). Edge computing as one of the trends. IEEE Computer, 50(1), 30-39.

https://doi.org/10.1109/MC.2017.9

[5] Zhang, C., & Fan, Z. (2021). Privacy and security implications in edge computing: A survey. ACM Computing Surveys, 54(3), Article 67. https://doi.org/10.1145/3453152

[6] Sardar, D., & Ghosh, S. K. (2021) Energy-efficient algorithms for IoT applications in edge computing: A case in point in industrial automation. Manufacturing smart contracts using state-of-art blockchain technologies for Industry 4.0 and Industrial IoT: A systematic review 2021 3rd IEEE International Conference on Industrial IoT and Edge Computing, 5139753, pp.101-110. IEEE. https:[Online]. Available at:< doi.org/10.1109/IIOT.2021.9486543

[7] Lin, Y., & Hu, L. (2019). Smart Cities and application of edge computing for real time data processing. Proceedings of the 2019 IEEE Conference on Edge Computing, Edge Computing [Internet] 77-84. IEEE. https:>Accessed October 2, 2021. doi:10.1109/EDGE.2019.00018

[8] Abadi, M., & Chen, J. (2019). Edge computing in IoT: A brief of trends and issues. Journal of IoT and Edge Computing vol 5 no 2 pp 25-38.

[9] Cisco Systems. (2020). The Future of IoT and Edge Computing: Towards smarter industry solutions. Cisco White Paper. Retrieved from https://www.cisco.com/

[10] OpenFog Consortium. (2017). This paper presents OpenFog Reference Architecture for Fog Computing. Retrieved from https:/* OpenFog Consortium

Resource*/.datasets.locateByType>/ www.openfogconsortium.org/resources