

A Comprehensive Review on Edge Computing for IoT with Emphasis on Security Challenges and Solutions

¹Sankeeta Jha, ²Abhishek Shahi and ³Jaspal Kumar

¹Department of Computer Science & Engineering, Echelon Institute of Technology, Faridabad, Haryana, India

²Department of Computer Science and Engineering, Buddha Institute of Technology, Gorakhpur, UP, India

³Department of Electronics and Communication Engineering, Echelon Institute of Technology, Faridabad, Haryana, India

jaspal@eitfaridabad.co.in, sankeetajha@eitfaridabad.co.in

Abstract

The field of computing is currently dealing with a dilemma between speed and scale. While the cloud provides unparalleled computing power and storage, transferring data to and from it takes time. To address this issue, a methodology called Edge Computing has emerged. This approach brings the cloud's capabilities closer to the devices that generate data, allowing for context-aware and time-sensitive services in the Internet of Things (IoT) era. Rather than relying solely on cloud computing, edge computing utilizes the power of local computing and nearby devices as edge servers to provide timely and intelligent services. This approach offers several benefits, including improved scalability and the use of customer computing abilities. However, there are still several challenges that need to be addressed, such as managing data storage and computing efficiently, integrating edge computing with cloud computing for scalable services, and ensuring the security of the entire system. This research paper aims to present a concise analysis of Edge Computing Architecture and System Design.

Keywords: Cloud computing, Edge computing, IOT, Security

ILLUSTRATIONS:

Introduction to Edge Computing:

Edge Computing is a distributed computing paradigm that brings computation and data storage closer to the sources of data. It aims to reduce latency, save bandwidth, and enable real-time data processing.

Architecture of Edge Computing:

The architecture of Edge Computing consists of three tiers: the cloud tier, the edge tier, and the device tier. These tiers work together to enable efficient and effective data processing, storage, and transmission.

Edge Computing Use Cases:

Edge Computing has a wide range of use cases, including but not limited to Industrial Internet of Things (IIoT), autonomous vehicles, smart cities, remote monitoring, and immersive entertainment.

Edge Computing Challenges:

The challenges associated with Edge Computing include security and privacy concerns, infrastructure and deployment complexities, and interoperability issues.

Edge Computing Technologies:

Edge Computing leverages various technologies, including but not limited to, 5G networks, Internet of Things (IoT) devices, Artificial Intelligence (AI), and Machine Learning (ML).

Edge Computing Standards:

Standardization is crucial for the successful implementation and deployment of Edge Computing. Various organizations, including the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI), are working towards developing standards for Edge Computing.

Edge Computing Future:

Edge Computing is expected to witness tremendous growth in the coming years. With the rise of 5G networks and IoT devices, Edge Computing is poised to revolutionize various industries and domains, including healthcare, manufacturing, and entertainment.

I. INTRODUCTION

Edge computing allows for the analysis of Internet of Things data at the edge of the system, before sending it to the data center or cloud. When multiple devices transmit data simultaneously, the quality of the data can suffer due to latency, and the bandwidth costs can be significant. Edge computing hardware and services provide a local source for processing and storing these systems, such as an edge gateway that can process data from an edge device and only send back the necessary information through the cloud, reducing bandwidth needs. Edge devices can include IoT sensors, laptops, smartphones, surveillance cameras, or even web-connected appliances like microwaves. Edge gateways themselves are considered edge devices within an edge computing system.

For many businesses, the cost savings alone can be a compelling reason to adopt edge computing. Companies that rely heavily on cloud-based applications may have found that bandwidth costs were higher than expected. However, the most significant advantage of edge computing is the ability to store and process data faster, enabling more productive real-time applications that are essential to businesses. Prior to edge computing, a phone performing facial recognition would need to run the test through a cloud-based service, which required significant processing effort. With an edge computing architecture, the calculation can run locally on an edge server, such as the phone itself. Applications such as virtual reality, self-driving cars, augmented reality, smart cities, and building automation systems require fast processing and response times, making edge computing crucial for their development.

II. LITERATURE SURVEY

In this paragraph, the content of several research papers on edge computing is summarized. The first paper discussed analyzed current edge computing systems and open projects based on their design requirements and innovations, while also addressing issues related to energy conservation and designing edge computing systems for deep learning. The second paper proposed a technique and conceptual structure for edge enabled IoT engineering task coordination using a bounded model for calculating coordination plans. The third paper discussed the feasibility of providing delay and reliability assurances for edge computing services and highlighted selected use cases that demonstrate the relationship between edge computing and ultra-reliable low latency communication. The fourth paper reviewed common attacks on edge computing systems and the security mechanisms that can be implemented to address them, as well as future directions for secure edge computing systems. Finally, the fifth paper provided a systematic analysis of current edge-based IoT security solutions within a formally specified edge-centric IoT architecture, including topics such as network infrastructure, intrusion detection systems, and designs that protect privacy.

III. EDGE COMPUTING SYSTEM DESIGN AND ARCHITECTURE

The passage provides an overview of IoT (Internet of Things) and the challenges associated with it. IoT involves connecting physical objects to the internet and enabling them to make smart decisions without human intervention. The advancements in IoT technologies include sensor systems, RFID, communication technologies, and internet protocols. IoT applications include logistics, manufacturing, healthcare, industrial automation, and emergency handling, which offer significant market opportunities.

10.48047/jocaaa.2024.33.08.631

ISSN:1521-1398 ,1572-9206

The analysis of data patterns predicts that the majority of IoT applications will require highly reliable and low-latency services from service providers. Reliability refers to the ability to ensure effective message transport within a simulated time interval, while latency refers to the time passed since the information is transmitted until it has reached the receiver side.

The passage highlights that the current network solutions are not adequate to support the needs of IoT, and new designs are required to provide smart functionalities to self-managing objects. Cloud computing, which is concentrated at a single place, may not be able to handle the growing traffic demands of IoT, resulting in significant delays and degraded network performance.

To address these challenges, edge computing models such as fog computing, mobile edge computing, and cloudlets have been proposed. These models bring service supply closer to the network edge, reducing latency and traffic intensity at the centralized network and lessening resource processing compared to traditional IoT models. However, a comprehensive approach is needed to improve the robustness of edge computing models for IoT to handle the changing attributes of various users and ensure data quality.

The proposed structure includes solutions at the physical, business layers, and networking applications to better the dependencies of a network. The increasing number of mobile devices provides options for a close network, reducing latency and interference, and increasing reliability and energy efficiency.

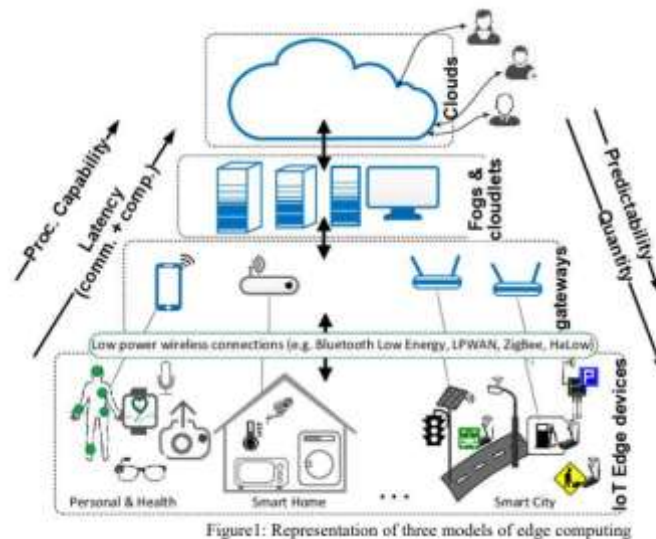


Figure1: Representation of three models of edge computing

The goal of IT is to develop a resilient and adaptable edge network for the Internet of Things. This structural plan involves implementing solutions at different levels to improve network strength to accommodate varying resource availability and to provide ubiquitous support for IoT.

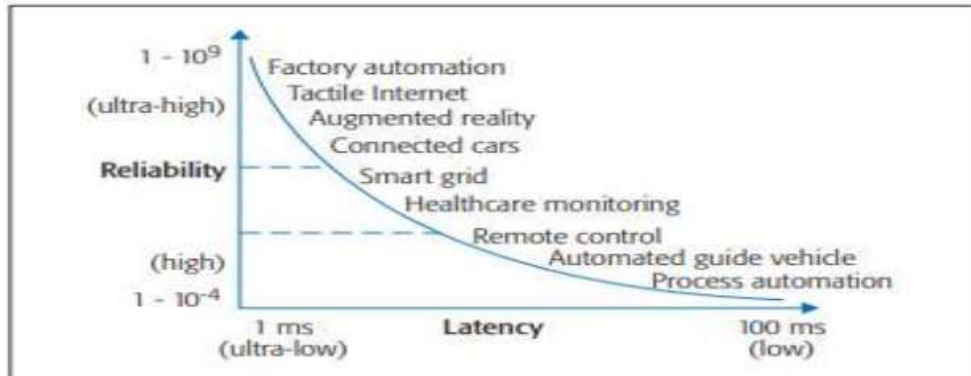


Figure2: Reliability and latency requirement in IOT

Figure 3 provides an overview of the three-tiered computing model consisting of IoT, edge, and cloud. The first layer is IoT, which includes devices such as drones, smart home tools and equipment, connected health sector devices, and commercial internet infrastructure. Various communication protocols are utilized to connect IoT with the edge. For instance, drones can be connected to a cellular tower using 5G/4G/LTE, while sensors in a smart home can interact with the home gateway through WiFi. The edge layer comprises connected and autonomous vehicles, edge servers, cellular towers, and gateways, which require the immense computational and storage capacities of the cloud to perform complex tasks. Communication protocols between IoT and edge generally consume lower energy and cover smaller distances, while those between edge and cloud have wide bandwidth and high speeds. The ideal protocols for communication between edge and cloud are Ethernet, optical fibres, and 5G which is latest.

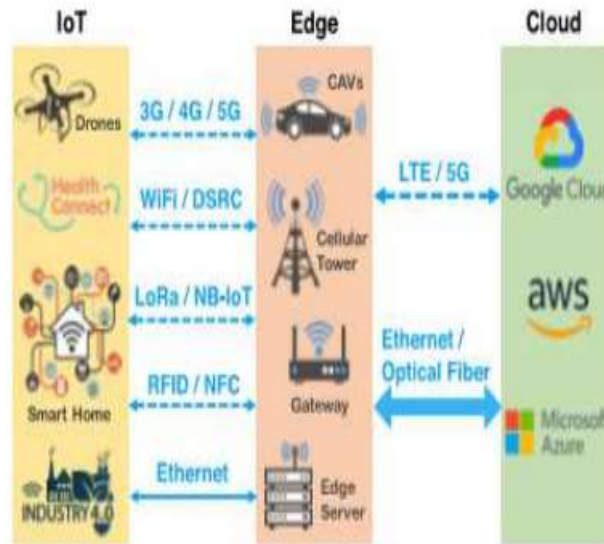


Figure 3: Reference architecture of Edge-IOT paradigm

IV. BENEFITS OF EDGE-IOT COMPUTING

It's no surprise that businesses are turning to cutting-edge solutions to tackle the challenges of cloud infrastructure. Edge data centers operate closer to the end user by placing bandwidth-intensive content and latency-sensitive devices near the data source. Unlike remote cloud computing, edge-driven applications operate on IoT devices without the need for electronically controlled metadata transfer to the cloud or other frameworks. In other words, data processing takes place exactly where the data is generated, managed, and stored on an IoT-based entity or subnetwork within a local network. IoT data can be sent to any number of IoT clouds through a programmable and extendable IoT Edge network that can be interpreted by almost any program. Smart Edge provides enormous potential benefits to the edge owner. The following points elaborate on the need for an edge computing framework for IoT:

a. Latency

Latency is a function of the time it takes for a packet of data to travel from its source to its endpoint. While transmission link is a significant consideration, edge computing operates on a more dispersed framework than cloud computing, eliminating the extra path to the cloud and offering real-time centralized control, attentiveness, and resilience. This handles congestion and traffic and provides delivery to the closest available end-user software and equipment. As you get closer to the edge node, latency tends to decrease. However, you cannot have low-latency edge devices without the necessary access to the data center and cloud up the hierarchy.

b. Scalability

Scalability and elasticity in IoT through edge computing allow companies to maximize their processing power by integrating IoT devices and edge data centers. It also eases the costs of profitability as each new model added does not impose extensive demands on a network's core bandwidth.

c. Security

The security features of IoT Edge Computing make the network nearly opaque to any disruption when handling, refining, and using programs across a wide range of platforms and data centers. Additionally, it keeps the data retained and processed within the device, ensuring maximum security.

d. Versatility

The ability to quickly modify the system layout through virtual tools and incorporate new features and software will be a crucial aspect of IoT edge devices. Moreover, all updates, packages, and controls must have improved protection to prevent threats as automated delivery becomes more prevalent. The aim is to enable a specialist without any knowledge or experience of IoT and IoT edge devices at a specific site to connect a power strip and a network cable, and then leave with automated authentication and provisioning software. If the system needs to be moved, the new position's specifications will be dynamically self-supplied to ensure that the process is as seamless as possible.

e. Cost Efficient

The cost factor plays a significant role in edge computing as well. In IoT applications, most of the telemetry data generated by sensors and actuators may not be essential. With edge computing, data can be filtered and analyzed before it is transmitted to the cloud, which reduces data transfer costs on the network. Furthermore, it reduces data storage and computational costs in the cloud that are not necessary for the application.

f. Reliability

Reduced data traffic and cloud storage can lead to increased productivity in commercial operations. Unlike other cloud-based IoT devices, link-related issues are not a major concern with edge computing. This is because edge-driven applications can operate independently, even in situations with poor or no internet connection, which in turn improves reliability automatically.

Capgemini has developed edge technologies that support manufacturers, making it easy to customize and extend "FD4 IoT Edge" for asset safety tracking, visual quality audits, and adaptive maintenance applications quickly. Azure IoT Edge is a service for the Internet of Things (IoT) that operates on top of the IoT Hub and enables consumers to perform edge computing. Edge computing is the processing of data on computers at the edge of the network rather than in the cloud itself.

V. CHALLENGES

The edge computing paradigm is impressive but faces several challenges in the near term, some of which are difficult to overcome.

a. Security: One of the most challenging issues with edge computing architecture and deployments is security. While holding data closer to the sensors where it is generated and used reduces the number of vectors of threat, fog clusters may be vulnerable to various forms of network-based and physical attacks due to their remote existence. Trusting hardware origins, interface components, and trusted execution environments will be crucial features of fog nodes to build a strong security foundation and extend it to applications up the stack.

b. Management: Another significant challenge facing fog deployments is management. As per projections, the number of connected IoT devices is expected to exceed 30 billion by 2030, overwhelming the edge nodes available today. Each edge node will handle traffic from 100 to 10,000 interconnected IoT devices, which means the deployment of between 30 million and 3 billion edge nodes over the next decade. This presents a significant obstacle for those responsible for building, configuring, and managing IoT networks on an ongoing basis.

c. Regulation: Edge computing and IoT network architecture lack standardized rules and regulations for system management, which is another challenge. While the US and UK Government agencies have established IoT rules and regulations, users are uncertain about how they apply specifically to their organizations. Without clear standards and general guidelines that legislation can provide, IT groups will not know how their IoT networks will look like or operate. In addition to IoT standards, IT decision-makers in their organizations also require BYOD policies and regulations to enable secure and productive implementation of disruptive technologies. Apart from these challenges, other obstacles may arise during Edge IoT implementation, such as network bandwidth, latency, performance, and data accumulation.

VI. CONCLUSION

Moving data analysis to the edge of the network can offer numerous benefits to companies, including improved performance and enhanced user experience, particularly with the rise in the number of IoT edge devices. It is estimated that approximately 25.4 billion such devices will be introduced by 2030, making this trend even more prevalent in the business world. By 2025, there will be 152,200 IoT devices connecting to the internet per minute. The amount of data generated by IoT devices is expected to reach 73.1 ZB (zettabytes) by 2025. Real-time computation is not feasible or efficient with traditional cloud methods, thus the network needs to be brought closer to the edge. In the telecommunications industry, there will be even more operators and IoT end devices with edge computing functionality and corresponding accuracy. The deployment of millions of IoT platforms and the adoption of AI/ML solutions is expected to generate economic

10.48047/jocaaa.2024.33.08.631

ISSN:1521-1398 ,1572-9206

value of around \$4-11 trillion by the end of 2025. Nevertheless, edge deployment is not without its challenges, which include trade-offs in structural complexity, efficiency, health, performance, time-to-service, and overall life process expenses. To address these challenges, effective edge deployments must be carefully analysed, and solutions must be devised.

References: -

- [1] Kumar, K. Suganya, G. (2018). Edge Computing Study Utilizing IOT Technologies. the third international conference on electronics and communication systems in 2018 (ICCES). Cite as: 10.1109/cesys.2018.8723950
- [2] Tsigkanos, C.; Dustdar, S.; and Murturi, I. (2019). Reliable Edge Resource Coordination at Runtime. IEEE Proceedings, 107(8), 1520–1536. Cite this URL: 10.1109/jproc.2019.2917314
- [3] Dan, G., and Josilo, S. (2019). Allocating Wireless and Computing Resources for Edge Computing's Selfish Computation Offloading. The 2019 IEEE Conference on Computer Communications is known as IEEE INFOCOM. Cite this URL: 10.1109/infocom.2019.8737480
- [4] Wang, S. (2019). Applications, state-of-the-art, and challenges of edge computing. Networking Advances, 7 (1), 8. 10.11648/j.net.201907.01.12
- [5] Yang, T. A., Wei, W., and Davari, S., Sha, K. (2019). a review of edge computing-based IoT security designs. Doi: 10.1016/j.dcan.2019.08.006 Digital Communications and Networks.
- [6] IoT (Internet of Things) - Real-world edge computing architectural challenges. (August 16, 2019). Citation taken from <https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-edge-computing-architecture.html>
- [7] Research Department at Statista (2016, November 27). IoT: the number of globally linked devices from 2012 to 2025. The information was collected from <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.
- [8] Tata, S., Jain, R. (2017). Distributed Deployment of Process-Aware IoT Apps from the Cloud to the Edge. International Conference on Edge Computing, 2017 IEEE (EDGE). Cite this URL: 10.1109/ieec.edge.2017.32
- [9] D. Jensen (2019). Key Ideas for Azure IoT Edge. Doi: 10.1007/978-1-4842-4536-1 2 "Starting Azure IoT Edge Computing," 17–47
- [10] Jacob, P., Nagarajan, G., A., P., and P. (2019). An extensive survey of edge computing for the internet of things. Advances in Computational Intelligence and Robotics, 37–45. doi: 10.4018/978-1-5225-8555-8.ch003. Edge computing and computational intelligence paradigms for the Internet of Things.

10.48047/jocaaa.2024.33.08.631

ISSN:1521-1398 ,1572-9206

[12] Nagarajan, G.; Minu, R. I. (2019). Edge Computing Can Close the IoT Gap. Advances in Computational, "Edge Computing and Computational Intelligence Paradigms for the IoT." doi: 10.4018/978-1-5225-8555-8.ch001

[13] Shapsough, S., Zualkernan, I. A., & Aloul, F. (2018). Low-Resource Edge Device Security in IoT Systems. (ISSI). Reference: 10.1109/issi.2018.8538135

[14] Bojan Jovanovic, (2023)., "Internet of Things statistics for 2023 – Taking Things Apart"