Evolution of Information, Communication and Computing Systems (EICCS)
https://publisher.uthm.edu.my/bookseries/index.php/eiccs

Trends and Challenges in Mobile Edge Computing for the Next Generation Massive Internet of Things

Muhammad Asif Khan[1]* and Mohd Anuaruddin Ahmadon[2]

[1]Qatar Mobility Innovations Center,
Qatar University, Doha, QATAR

[2]Graduate School of Sciences and Technology for Innovations,
Yamaguchi University, 16-1-2 Tokiwadai, Ube, Yamaguchi, 755-8611, JAPAN

*Corresponding Author

Abstract:
Mobile Edge Computing (MEC) is a novel computing paradigm that brings data storage and computing resources closer to the end-users (i.e., at the network edge). The proximity between end users and the edge servers enables efficient access to data storage and faster processing, reduced network latency, and improved Quality of Service (QoS). The integration of MEC with the Next Generation Massive Internet of Things (MIoT) has the potential to solve several challenges such as scalability, reliability, and security of IoT systems but also enables unprecedented novel use cases. This chapter explores the current trends and challenges in MIoT and MEC, the benefits of their integration, and the state-of-the-art techniques used to achieve MEC-enabled MIoT systems. The chapter also discusses the potential applications and use cases of MEC for MIoT, including smart cities, industrial automation, and healthcare.

Keywords:
Edge computing · Internet of Things · MEC · Massive IoT · 5G · 6G

1. Introduction

The Internet of Things (IoT) has emerged as a disruptive technology, providing new opportunities for businesses, governments, and individuals. IoT devices collect, transmit, and process vast amounts of data, enabling unprecedented new applications and services. However, the growth of IoT has also created new challenges, including scalability, reliability, and security. In many scenarios, IoT devices leverage cloud computing infrastructures for data storage and processing. In cloud computing, all data from IoT devices is sent to centralized servers for processing and analysis, which is often inadequate to support the scale and real-time requirements of IoT applications due to high network latency, bandwidth limitations, and security concerns.

To address these challenges, Mobile Edge Computing (MEC) has emerged as a promising solution that brings computing, storage, and network resources closer to IoT devices, enabling faster and efficient data processing, reduced network latency, and improved Quality of Service (QoS).

**Corresponding author: asifk@ieee.org*

In this chapter, we will explore the role of MEC in the next generation of IoT, known as Massive IoT (MIoT). The integration of MEC with MIoT has the potential to enhance the scalability, reliability, and security of IoT systems. We will first provide an overview of MIoT and the unique challenges it presents. Next, we will discuss the key concepts and architecture of MEC and its potential benefits for MIoT. Finally, we will examine some use cases and applications where MEC can be applied to address the challenges of MIoT where MEC can be applied to address the challenges of MIoT.

2. Massive Internet of Things (MIoT)

The Next Generation Massive Internet of Things (MIoT) is an emerging field that promises to connect billions of devices and sensors, enabling a wide range of applications in various domains such as healthcare, agriculture, transportation, and smart cities. With a projection of over 75 billion connected devices by 2025 [1], the number of devices and data generated far exceeds the capacity of traditional cloud computing architectures. In the field of Massive Internet of Things (MIoT), there are a variety of trends. Concerns regarding IoT cybersecurity, advancements in healthcare, and 5G facilitating more IoT opportunities are among the most significant drivers and innovations in this field. Globally, roughly 29 billion of these devices will be connected to the internet by 2022. The healthcare industry has been one of the most prominent in IoT development, encompassing everything from social distance monitoring to telemedicine and remote healthcare. It is anticipated that 5G mobile networks will be the next significant advancement in mobile broadband. When peak speeds for downloading reach as much as 20 gigabits per second, it will be possible to perform specialized tasks such as remote precision medicine, linked vehicles, virtual and augmented reality, and a wide range of Internet of Things (IoT) applications. 5G will be able to accommodate the massive number of devices that will be connected to the network concurrently. This number will be significantly greater than what 4G LTE can support. Because 5G enables MIoT applications, such as those in the fields of medicine, education, energy, and transportation, it is crucial that these applications perform as expected, uninterrupted, and without exception.

The challenges of MIoT are numerous, including three major challenges i.e., scalability, reliability, and security. These are discussed below:

2.1 Scalability

MIoT systems need to support the connection and management of a large number of devices and sensors. Scalability is a critical challenge in MIoT, as traditional cloud computing architectures are ill-suited to handle this volume of data, leading to issues such as high latency and network congestion. Additionally, MIoT devices are often deployed in remote or harsh environments, where network connectivity and power are not always reliable. The high-volume, high-velocity, and high-variety characteristics of MIoT-based big data present challenges for data discovery, convergence, heterogeneous connectivity, and extraction processes. The magnitude and degree of complexity of data create new conditions for data processing, and the diversity of data sources also poses a risk.

2.2 Reliability

MIoT systems need to be reliable and provide consistent QoS to meet the needs of various applications. The reliability of MIoT systems depends on several factors, such as the robustness of the communication network, the availability of resources, and the reliability of the devices and sensors. Many MIoT applications require low latency and high throughput, such as autonomous vehicles and industrial automation systems. Traditional cloud computing architectures are not designed to handle such requirements, as data must be sent to centralized servers for processing, leading to high latency and network congestion. Reliability is one of the primary obstacles that must be overcome to enable the Internet of Things (IoT)-enabled transformation of human society into one that is smart, practical, and effective with the potential for immense economic and environmental benefits. One example is energy conservation. Energy conservation techniques are essential for attaining high reliability in Internet of Things (IoT) services, particularly in the Massive IoT (MIoT), which requires battery-powered devices to have a low cost and energy consumption.

2.3 Security and Privacy

MIoT systems need to ensure the security and privacy of the data generated by devices and sensors. The proliferation of IoT devices and sensors increases the attack surface, making MIoT systems vulnerable to various security threats such as malware, DDoS attacks, and data breaches. Ensuring the security and privacy of MIoT systems is critical to prevent unauthorized access, data leakage, and other security. IoT devices lack the computational power and memory to implement robust security mechanisms. Additionally, the sheer number of devices and the heterogeneity of the devices and protocols used make it difficult to implement a unified security architecture. There are significant concerns over the protection of users' personal information and data in the IoT. The increased amount of data processed by devices connected to the Internet of Things (IoT) brings with it an increased risk of exposing personally identifiable information and other confidential data. There are several important considerations about the safety and confidentiality of the data that is gathered by IoT devices, regardless of whether the information is being sent or kept in the cloud.

3. Mobile Edge Computing

MEC is a distributed computing architecture that brings computation and data storage closer to the end-users and devices, enabling low-latency, high-throughput applications. MEC was first introduced and defined by the European Telecommunications Standards Institute (ETSI) as a technology which “provides information technology (IT) and cloud computing capabilities at the edge of the mobile network, within the Radio Access Network (RAN) in close proximity to mobile subscribers” [2]. In MEC, edge servers are deployed in close proximity to the end-users and devices, providing a more efficient and scalable computing platform. MEC is built on three key concepts: edge computing, network slicing, and virtualization.

Edge computing involves moving computation and storage closer to the end-users and devices. This reduces the latency and network congestion caused by sending data to centralized cloud servers. Edge computing enables real-time processing and analysis of data, which is critical for many MIoT use cases. Edge computing is widely used to assist activities such as predictive maintenance, energy efficiency, individualized production cycles, automated manufacturing, and smart operations. Industrial leaders use the edge to monitor, analyze, and manage energy usage in their factories, plants, and offices. They also utilize the edge as part of an IoT ecosystem. This includes using the edge to monitor, analyze, and manage energy consumption in their factories, plants, and offices.

Network slicing allows for the creation of dedicated, virtualized network resources enabling customized network configurations and resource allocation based on the specific needs of the users. The 3GPP release 16 defines dedicated network slice for MIoT application [3]. Network slicing enables the creation of separate logical networks for different applications, which ensures the isolation of traffic and resources. The method of network slicing offers a variety of advantages. It enables resource and security separation, predictable latency, flexible topology connection modification, automated slice management, and many more capabilities. The processing of data prior to its transmission across the

WAN is one way that network slicing may assist in cost reduction. This enables businesses to spend less money on bandwidth.

Virtualization allows for the creation of virtualized instances of hardware and software resources, providing a more flexible and scalable computing platform. Virtualization enables the creation of virtual machines and containers, which can be dynamically provisioned and managed. This provides greater agility and scalability for MIoT applications.

3.1 Architecture of MEC

The architecture of MEC consists of four layers: the device layer, the radio access network (RAN) layer, the edge computing layer, and the cloud computing layer (depicted in Figure. 1). The device layer includes all the MIoT devices and sensors that generate data. These devices can be connected to the edge servers via wired or wireless networks. The RAN layer includes the base stations and access points that connect the devices to the edge servers. This layer is responsible for managing the wireless connections and ensuring that data is transmitted efficiently and securely. The edge computing layer includes the edge servers that are deployed in close proximity to the devices. These servers provide the computing and storage resources required for MIoT applications. Edge servers can be deployed in a variety of locations, including cell towers, data centers, and enterprise premises. The cloud computing layer includes the centralized cloud servers that provide additional computing and storage resources for MIoT applications. Cloud servers can be used for tasks that require more computing power and storage than edge servers can provide.

MEC architecture enables the distribution of computing resources across multiple layers, providing a more efficient and scalable computing platform for MIoT applications. MEC has the ability to increase the performance of MIoT applications as well as minimize latency thanks to its distribution of computing resources across many levels. This is due to the fact that data may be processed nearer to where it is created, hence decreasing the need for data to travel great distances to a central cloud in order to be processed there.

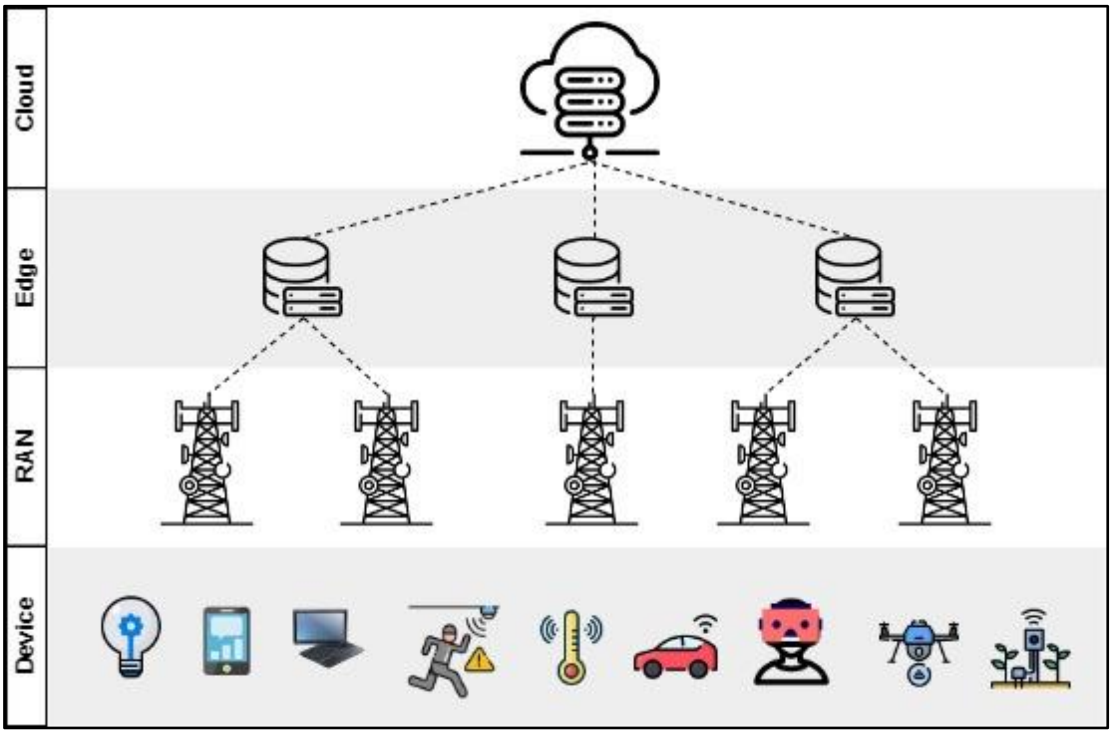

Figure 1: Architecture of Mobile Edge Computing (MEC)

3.2 Benefits of MEC

The primary benefit of MEC is to reduce the communication and computational latency incurred during the data transfer between the end users and the server. A simple analysis of edge computing is presented in this section. Consider an IoT device needs to process a task (e.g., transcoding a video chunk, running a classifier model etc.). If the IoT task performs the task locally, the local computational time is calculated in Eq. 1 [4][5]:

$$D_{local} = \frac{L_i C}{F_i} \quad \forall i \in N \tag{1}$$

The total edge computing delay $\mathrm{D_{edge}}$ is comprised of the communication delay D_{comm} and the processing or computation delay D_{comp}.

$$D_{edge} = D_{comm} + D_{comp} \tag{2}$$

$$D_{comm} = \frac{1}{R} = \frac{1}{W\, log_2(1+\frac{P_e|h_e|^2}{N_i})} \quad \forall i \in N \tag{3}$$

$$D_{comp} = \frac{L_i C}{F_e} \quad \forall i \in N \tag{4}$$

Where in Eq. 3, R is the data rate between RAN (where the edge server is located) and the end device, W is the bandwidth of the wireless channel, P_e is the transmit power of the edge server (considering the downlink transmission, for uplink transmission this can be the transmit power of the device), h_e is the channel gain, and N_i is the noise power (i represent the end device). In Eq. 4, L_i represents the size of the computational tasks requested by user i (usually in bits), C is the CPU cycles required on the edge server to process one bit, and F_e is the computational power of the edge server (in cycles per second).

Using the analysis above, a user can take different approaches to process the tasks. For instance, if there is a delay constraint (in real-time applications) on the task, the user may decide to offload the task to the edge server if $D_{edge} < D_{local}$. Typically, edge-based services are expected to guarantee QoS using the network slicing approach. Similarly, if the $D_{comp} \gg D_{comm}$, the user may prefer to offload the task to for edge computing and vice versa. In some cases, a user may decide between local and edge computing mode based on the energy consumption to save local battery resource [6].

Fig. 2 presents an analysis of inference delay while computing a deep learning image classification model (VGG-16) in an edge-assisted generic IoT network (the edge server is amazon web services (AWS) C5n server). The model is run in a distributed manner i.e., the model layers are distributed among the IoT device and the edge server. One can observe that the total inference delay increases when more layers are executed locally). By placing computing power and storage closer to the edge of the network, where data is created and consumed, we may increase inference performance by using edge computing. This is because edge computing brings processing power and storage closer to the edge of the network. This has the potential to lower latency and enhance the performance of applications that need the processing of data in real time. In the case of a deep learning image classification model, for instance, edge computing may make it possible for the model to be run in a distributed fashion. In this scenario, certain layers of the model may be implemented on the IoT device, while others may be done on an edge server. This may cut down on the quantity of data that has to be sent to a centralized cloud for processing, which in turn can improve inference speed and minimize the amount of latency experienced.

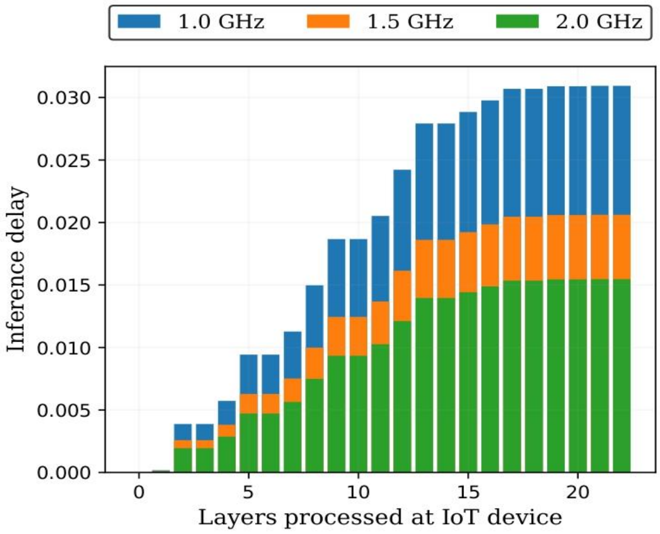

Figure 2: Inference delay using Edge Computing

MEC has several potential benefits for MIoT. First, MEC enables low-latency, high-throughput applications, which are critical for many MIoT use cases. Second, MEC provides a more efficient and scalable computing platform, enabling MIoT applications to scale to support the massive number of devices and data generated. Finally, MEC provides a more secure computing platform, as edge servers can implement robust security mechanisms to protect against cyber threats.

3.2.1 Low-latency, High-throughput Applications

MEC enables low-latency, high-throughput applications, which are critical for many MIoT use cases such as autonomous vehicles, robotics etc. In such use cases, a huge amount of data needs to be transmitted from the data server to the device which incurs a large amount of network delay. Thus, using MEC, the data is proactively cached at the MEC server to provide faster access to the end user

[7][8]. By moving computation and storage closer to the devices, MEC reduces the latency and network congestion caused by sending data to centralized cloud servers. This enables real-time processing and analysis of sensors data, which is critical for applications such as autonomous vehicles and industrial automation systems.

3.2.2 Scalability

MEC provides a more efficient and scalable computing platform for MIoT applications. By distributing computing resources across multiple layers, MEC enables MIoT applications to scale to support the massive number of devices and data generated. Additionally, MEC enables dynamic provisioning and management of resources, providing greater agility and scalability for MIoT applications [9][10][11]. MEC uses the concept of network slicing to enable isolated virtual networks to deploy different services using Network Function Virtualization (NFV). Thus, different MIoT network slices can be deployed to guarantee the service-specific quality of service (QoS) in large scalable MIoT networks, without affecting the QoS delivered to each network slice.

3.2.3 Security

MEC provides a more secure computing platform for MIoT applications. IoT devices are generally produced with weak encryption and encoding schemes to maintain an affordable price to compete in the market. Hence, IoT networks are most vulnerable to several security threats. Edge servers can thus employ robust security mechanisms to protect against cyber threats. Using network slicing, network operators can create separate logical networks for different IoT applications, ensuring the isolation of traffic and resources enhancing the security of MIoT applications. MEC also keeps the data local, enabling more control over the data as compared to cloud computing in which the data is stored on the remote cloud servers needs to be transmitted to the Internet [12][13]. MEC also introduces multi-server collaboration to eliminate single-point redundancy as in most cloud environments [9].

Fig. 3 summarized the benefits of MEC. MEC can improve the scalability of applications by enabling them to handle more data and users. MEC can also improve security by enabling data to be processed locally, reducing the need to transmit sensitive data over the network. By reducing the distance that data needs to travel, MEC reduces latency and improves the performance of real-time applications.

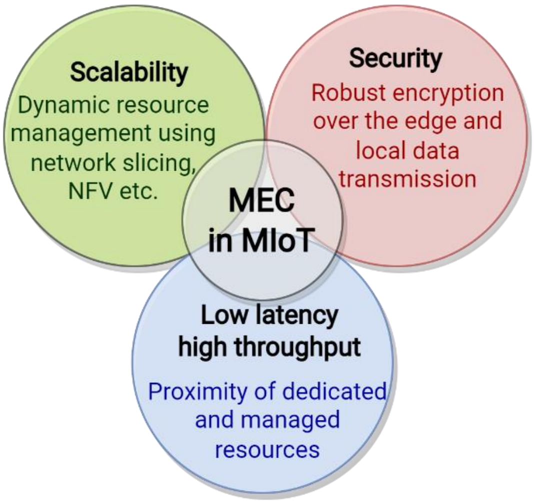

Figure 3: Benefits of MEC

4. Use Cases and Applications of MEC for MIoT

MEC can be applied to a variety of MIoT use cases and applications. Some examples include:

4.1 Autonomous Vehicles

Autonomous vehicles require low-latency, high-throughput applications to operate safely and efficiently. MEC enables real-time processing and analysis of IoT data from sensors on the vehicle, such as cameras, LiDAR, and radar. This allows the vehicle to make decisions in real-time, such as identifying and avoiding obstacles, and communicating with other vehicles and infrastructure. MEC can also enable edge-based machine learning algorithms that can improve the accuracy and performance of autonomous vehicle systems [14][15]. There is a growing interest in the area of edge-AI for autonomous vehicle applications and MEC provides a platform to enable such deployments. Fig. 4 illustrates an example in which an autonomous vehicle offloads real-time data to an MEC server located ta the nearest base station and the MEC server performs the computational extensive tasks (such as running deep learning models) and transmit the final output to the car, the car uses this information to take a control action.

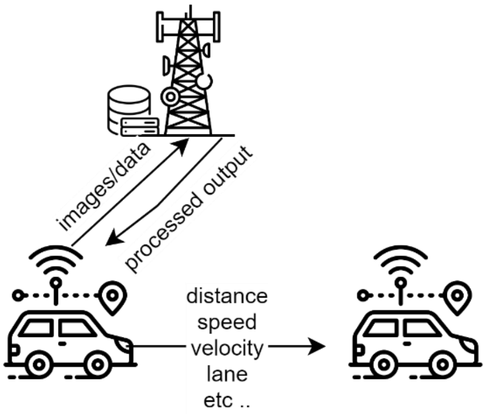

Figure 4: MEC in autonomous vehicles

4.2 Smart Cities

Smart cities can benefit from MEC in several ways. MEC can enable real-time monitoring and control of city infrastructure, such as traffic lights, parking meters, and waste management systems. This can improve the efficiency and effectiveness of city services and reduce costs. MEC can also enable the deployment of intelligent transportation systems, which can improve traffic flow, reduce congestion, and enhance safety [16]. Fig. 6 illustrates the use of MEC in smart cities by providing using a unified platform for big data analytics of smart cities management.

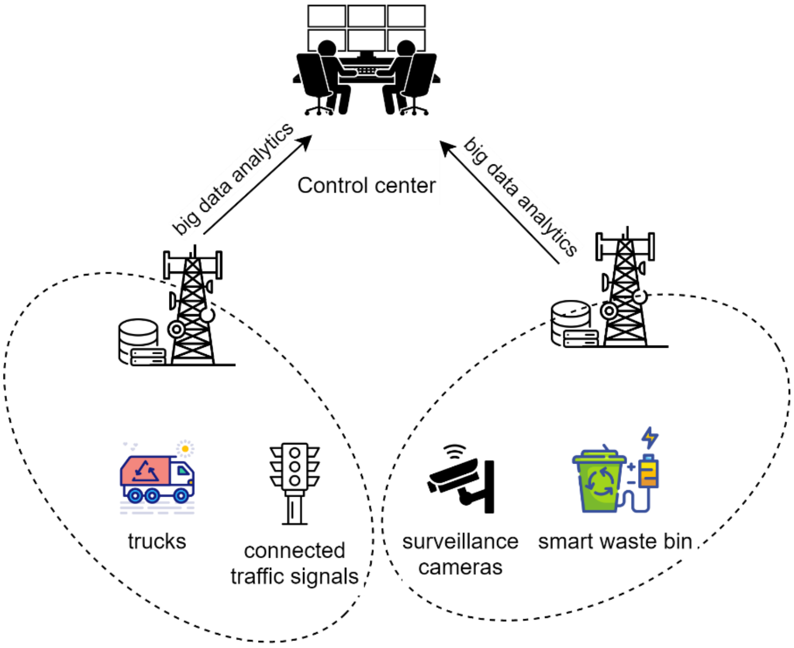

Figure 5: MEC in smart cities

4.3 Industrial Automation

Industrial automation systems involve low-latency, high-throughput MIoT applications that operate efficiently and safely. MEC can enable real-time monitoring and control of industrial processes, such as manufacturing lines and assembly plants [17]. This can improve the efficiency and productivity of industrial operations and reduce costs. MEC can also enable the deployment of predictive maintenance systems, which can detect and diagnose equipment failures before they occur, reducing downtime and maintenance costs [18].

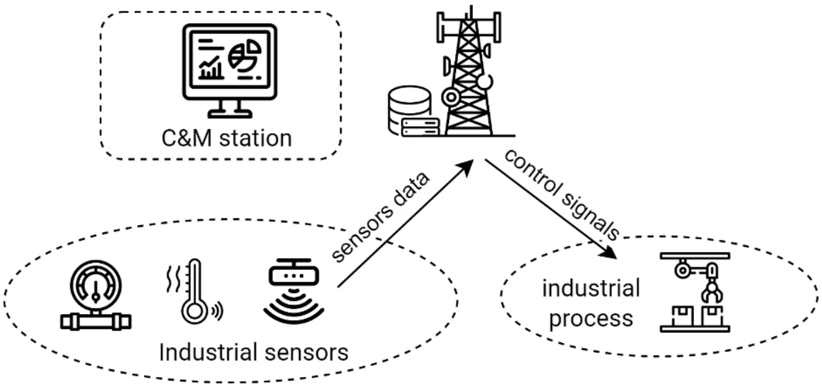

Figure 6: MEC in industrial automation

4.4 Healthcare

MEC can enable real-time monitoring and analysis of healthcare data, such as patient vital signs, medical imaging, and electronic health records. This can improve the quality of patient care and enable remote patient monitoring. MEC can also enable the deployment of personalized medicine systems, which can use machine learning algorithms to analyze patient data and provide personalized treatment plans. MEC can be applied to a variety of healthcare use cases, including remote patient monitoring, telemedicine, and personalized medicine [19]. In these applications, MEC enables real-time processing and analysis of data, which is critical for healthcare applications. This enables faster decision-making and response times, which can improve patient outcomes and reduce healthcare costs [20]. Fig. 7 illustrates a remote robotic surgery use case of MEC in which MEC servers collaborates to provide the required QoS such as ultra-reliable low latency communication (URLLC) to transmit and process the sensors data and command messages with high reliability.

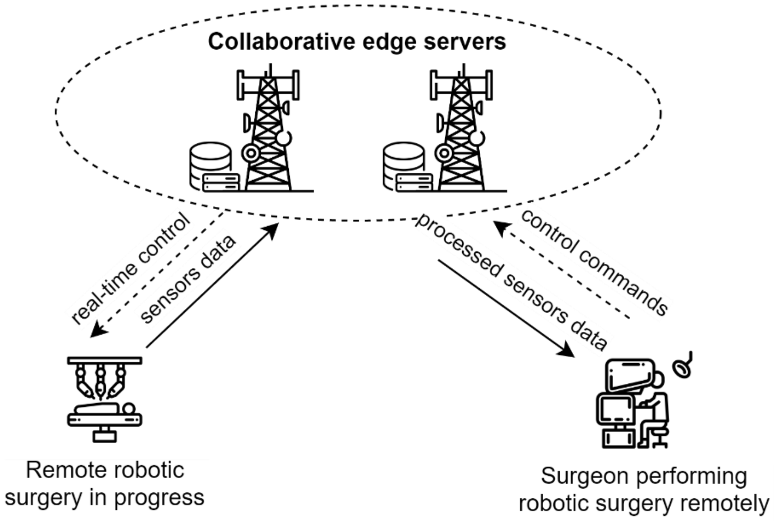

Figure 7: MEC in healthcare (A Use Case of Remote Robotic Surgery)

4.5 Smart Grids

Smart grid refers to the use of information and communication technologies (ICT) to improve the efficiency, reliability, and security of power grids. The key enablers for smart grid systems include Internet of Things (IoT) and machine learning (ML). Together MIoT and ML can enhance the performance of power system entities in smart grid operations such as event data acquisition and analysis, load forecasting, fault analysis and isolation, etc. Smart grid systems enabled with MIoT generate continuously huge amounts of data which must be stored and analyzed in real-time.

The transmission of the huge amount of data requires low-latency, high-throughput applications for efficient and reliable operations of smart grids. Thus, MEC can play a vital role in storing the data locally and analyze in real-time to implement necessary operations such as monitoring of electrical equipment, grid data analytics, etc. By moving computation and storage closer to the devices, MEC reduces the latency and network congestion caused by sending data to centralized cloud servers. This enables faster decision-making and response times, which is essential to ensure the efficient operation of smart grids [21]. Fig. 8 depicts a scenario in which MEC server receives real-time power generation and consumption data to perform tasks such as demand forecasting and load balancing. MEC server implement several necessary functions such as business intelligence models, demand forecasting models, and load balancing functions for reliable and efficient operations.

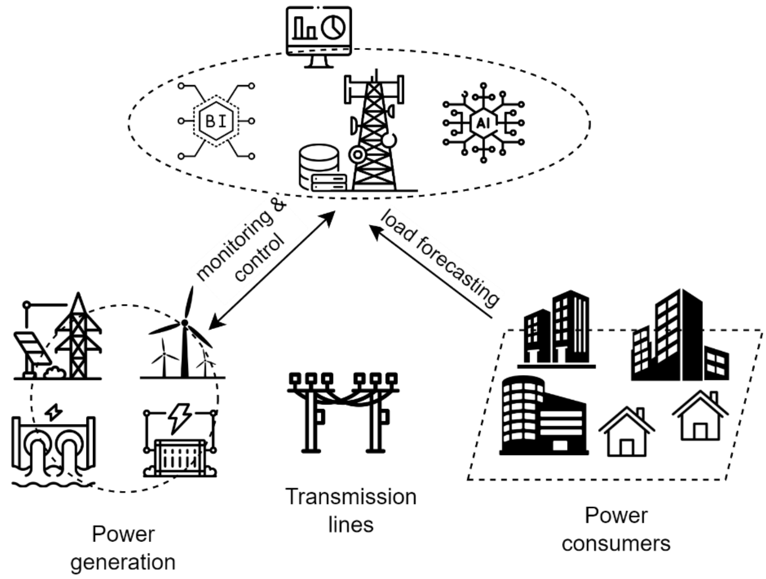

Figure 8: MEC in smart grid operations

5. Challenges and Limitations of MEC for MIoT

MEC deployment is still evolving, and practical deployment of MEC-enabled MIoT systems may face several real-world challenges [9][22][23].

5.1 Standardization

MEC is a relatively new technology, and there is currently a lack of standardization in the industry. Although 3GPP includes MEC in its latest release [3], the implementation may vary in practical deployment. This can make it difficult for MIoT developers to create interoperable solutions that can work across different MEC deployments. Standardization efforts are underway, but it will take time for a comprehensive set of standards to emerge [24].

5.2 Interoperability

Interoperability is a critical challenge for MEC. MIoT applications may use different communication protocols, data formats, and software frameworks, making it difficult to integrate and deploy MIoT applications across different MEC platforms. Standardization efforts are underway to address this challenge, but further work is needed to ensure interoperability between MEC platforms and MIoT applications [25].

5.3 Scalability

MEC enables greater scalability for MIoT applications, but there are still limitations to how many devices and data can be supported by the system. As the number of MIoT devices continues to grow, it will become increasingly challenging to provide sufficient computing and storage resources at the edge [4][6].

5.4 Resource Management

Resource management is a key challenge for MEC. MIoT applications may require different computing and storage resources, and these resources may need to be dynamically provisioned and managed based on the specific needs of the application [6]. This requires advanced resource management techniques, such as machine learning algorithms and autonomic computing, to ensure that MIoT applications receive the resources they need to operate efficiently [9].

5.5 Security and Privacy

Security and privacy are critical challenges for MEC. MIoT applications may generate sensitive data, such as personal health information or industrial trade secrets, which must be protected from cyber threats. MEC platforms must implement robust security mechanisms, such as encryption, access control, and intrusion detection, to ensure the security and privacy of MIoT applications. MEC provides a more secure computing platform for MIoT applications, but there are still potential security risks that must be addressed [12][13]. Edge servers can implement robust security mechanisms to protect against cyber threats, but they are still vulnerable to attacks. Additionally, network slicing can create security vulnerabilities if not implemented properly.

5.6 Cost

MEC requires the deployment of edge servers, which can be expensive to install and maintain. Additionally, the increased complexity of the system can result in higher operational costs. This can make MEC less cost-effective for some MIoT use cases, particularly those with low processing and storage requirements.

6. Future Directions

MEC is still a relatively new technology, and there are many areas for future development and research. Some possible directions for MEC in MIoT include:

6.1 AI and Machine Learning at the Edge

MEC can enable the deployment of AI and machine learning (ML) algorithms at the edge, which can significantly improve the efficiency and effectiveness of MIoT applications [26]. By performing data processing and analysis at the edge, MIoT devices can quickly respond to changing conditions and adapt to new situations. This can be particularly beneficial for applications such as autonomous vehicles, where real-time decision-making is critical.

6.2 Edge-to-Edge Collaboration

MEC can enable edge-to-edge collaboration, where multiple edge servers work together to process and analyze data. This can be particularly beneficial for MIoT applications that require complex processing, such as video analytics or natural language processing. By distributing the processing load across multiple edge servers, MIoT applications can achieve greater scalability and reliability [27].

6.3 D2D-Edge Collaboration

MEC emerged as a solution to meet the increasing storage and computing demand of future networks and services. However, deploying MEC servers at the RAN may not be sufficient alone to cope with the unprecedented demands of the future applications particularly in dense IoT deployments. A novel direction to solve this challenge is to utilize the distributed resources of capable IoT devices by using device-to-device (D2D) communication. Edge servers can thus not only collaborate with other edge servers but also IoT devices with unused processing resources to improve the overall system performance. Several D2D-MEC systems have been proposed in the literature that solve the challenge of limited edge resources in events of heavy demands. [4][5].

6.4 Integration with Blockchain

MEC can be integrated with blockchain technology to create secure and decentralized MIoT systems [28]. Blockchain can provide a tamper-proof record of MIoT data and transactions, which can improve security and trust in MIoT applications. Additionally, blockchain can enable new business models and revenue streams for MIoT applications, such as micro-payments for data sharing.

6.5 Energy Efficiency

MEC can be optimized for energy efficiency, which is critical for MIoT applications that rely on battery-powered devices. By reducing the amount of data sent over the network and minimizing the processing load on MIoT devices, MEC can extend the battery life of these devices [6][29][30]. Additionally, MEC can enable the use of renewable energy sources, such as solar or wind power, to power edge servers.

7. Conclusion

MEC is a powerful technology that can significantly improve the performance and efficiency of MIoT applications. By moving computation and storage closer to MIoT devices, MEC reduces latency, improves reliability, and enables real-time processing and analysis of data. MEC can be applied to a variety of MIoT use cases, including autonomous vehicles, industrial automation, smart grids, healthcare, and smart cities. Despite the many benefits of MEC for MIoT, there are several challenges and limitations that must be addressed, such as standardization, scalability, security, and cost. However, these challenges can be overcome with continued research and development. The future of MIoT is closely linked to the future of MEC, and we can expect to see many exciting developments in this space in the coming years.

References

[1] Sam Lucero, “IoT Platforms: Enabling the Internet of Things.”, white paper, 2016.

[2] Hu YC, Patel M, Sabella D, Sprecher N, Young V., “Mobile edge computing—A key technology towards 5G”, ETSI white paper. Sep 5;11(11):1-6., 2015

[3] Frederic Launay, "NG-RAN Network – Functional Architecture," in NG-RAN and 5G-NR: 5G Radio Access Network and Radio Interface, Wiley, 2021, pp.1-29.

[4] M. A. Khan, E. Baccour, A. Erbad, R. Hamila and M. Hamdi, "CODE: Computation Offloading in D2D-Edge System for Video Streaming," IEEE Systems Journal, pp. 1-12, 2022.

[5] Y. He, J. Ren, G. Yu, and Y. Cai, “D2d communications meet mobile edge computing for enhanced computation capacity in cellular networks,” IEEE Transactions on Wireless Communications, vol. 18, no. 3, pp. 1750–1763, 2019.

[6] M. A. Khan, R. Hamila, A. Erbad and M. Gabbouj, "Distributed Inference in Resource- Constrained IoT for Real-Time Video Surveillance," in IEEE Systems Journal, vol. 17, no. 1, pp. 1512-1523, March 2023

[7] G. S. Park and H. Song, “Video quality-aware traffic offloading system for video streaming services over 5g networks with dual connectivity,” IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 5928–5943, 2019.

[8] Y. He, J. Ren, G. Yu, and Y. Cai, “Joint computation offloading and resource allocation in d2d enabled mec networks,” in ICC 2019 – 2019 IEEE International Conference on Communications (ICC), pp. 1–6, 2019.

[9] M. A. Khan, E. Baccour, Z. Chkirbene, A. Erbad, R. Hamila, H. Hamdi, and M. Gabbouj, "A Survey on Mobile Edge Computing for Video Streaming: Opportunities and Challenges," in IEEE Access, vol. 10, pp. 120514-120550, 2022

[10] Tonini, Federico et al. “Scalable Edge Computing Deployment for Reliable Service Provisioning in Vehicular Networks.” J. Sens. Actuator Networks 8, 51., 2019

[11] Lin, Ying-Dar et al. “Scalable Mobile Edge Computing: A Two-Tier Multi-Site Multi-Server Architecture with Autoscaling and Offloading.” IEEE Wireless Communications, 28, 168-175, 2021

[12] Ranaweera, Pasika Sashmal et al. “Survey on Multi-Access Edge Computing Security and Privacy.” IEEE Communications Surveys & Tutorials 23, 1078-1124, 2021

[13] Ali, Belal et al. “Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review.” IEEE Access 9, 18706-18721, 2021

[14] A. Shakarami, A. Shahidinejad, and M. Ghobaei-Arani, “An autonomous computation offloading strategy in Mobile Edge Computing: A deep learning-based hybrid approach.” J. Netw. Comput. Appl. 178, 102974., 2021

[15] A. Jiao, and L. Ziliang, “Autonomous Driving Task Offloading with Mobile Edge Computing.” 2021 2nd International Conference on Computing and Data Science (CDS), 416-420., 2021

[16] Y. He, F. R. Tu, N. Zhao, C. M. Leung, and H. Yin, “Software-Defined Networks with Mobile Edge Computing and Caching for Smart Cities: A Big Data Deep Reinforcement Learning Approach.” IEEE Communications Magazine 55, 31-37, 2017

[17] Y. Chen, Z. Liu, Y. Zhang, Y. Wu, X. Chin, and L. Zhao. “Deep Reinforcement Learning-Based Dynamic Resource Management for Mobile Edge Computing in Industrial Internet of Things.” IEEE Transactions on Industrial Informatics 17, 4925-4934, 2021

[18] V. Díaz, J. Chun-wei Lin, and J. A. M. Molinera, “Introduction to the Special Section on Edge Computing AI-IoT Integrated Energy Efficient Intelligent Transportation System for Smart Cities.” ACM Transactions on Internet Technology 22, 1 – 2, 2022

[19] T. M. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, “Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT.” GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 1-6, 2020

[20] Z. Xue, P. Zhou, Z. Xu, X. Wang, Y. Xie, X. Ding, and S. Wen, “A Resource-Constrained and Privacy-Preserving Edge-Computing-Enabled Clinical Decision System: A Federated Reinforcement Learning Approach.” IEEE Internet of Things Journal 8, 9122-9138, 2021

[21] W. Wang, J. Yao, W. Zheng, and W. Shao, "Offloading Strategies for Mobile Edge Computing Based on Multi-Attribute Preferences in Smart Grids." 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC) 6, 1020-1024, 2022

[22] L. Qin, H. Lu, and F. Wu, "When the User-Centric Network Meets Mobile Edge Computing: Challenges and Optimization." IEEE Communications Magazine 61, 114-120, 2023

[23] A. K. Singh, S. C. Satapathy, A. Roy, and A. A. Gutub, "AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope." Arabian Journal for Science and Engineering,1-31, 2022

[24] A. S. Patel, P. Gandotra, R. Kumar, A. A. Khernai, B. Lall, and S. Mukherjee, "Standardization aspects of Tactile applications on Multi-access Edge Computing." 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), 899-904, 2022

[25] J. Casademont, B. Cordero, D. Campus-Mur, L. A. Moraise, A. S. Lalos, C. Vitale, C. Laoudias, and P. S. Khodashenas, "Multi-Radio V2X Communications Interoperability Through a Multi-Access Edge Computing (MEC)." 2020 22nd International Conference on Transparent Optical Networks (ICTON), 1-4, 2020

[26] P. K. Chandrika, M. S. Mekala, and G. Srivastava, "Edge resource slicing approaches for latency optimization in AI-edge orchestration." Cluster Computing 26, 1659 – 1683, 2022

[27] E. Baccour, A. Erbad, K. Bilal, M. A, Guizani, "Pccp: Proactive video chunks caching and processing in edge networks" Future Generation Computer Systems. Apr 1;105:44-60, 2020

[28] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, R. Hamila, Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. Computers & Security., Oct 1;109:102393, 2021

[29] Z. Sun, M. Zhao, and M. R. Nakhai, "Computation Offloading in Energy Harvesting Powered MEC Network." ICC 2021 - IEEE International Conference on Communications, 1-6., 2021

[30] H. Wang, Z. Lin, and T. Lv, "Energy and Delay Minimization of Partial Computing Offloading for D2D-Assisted MEC Systems." 2021 IEEE Wireless Communications and Networking Conference (WCNC), 1-6, 2021