

INTEGRATING IOT WITH 5G AND EDGE COMPUTING

Abstract

This chapter explores how IoT, 5G, and Edge Computing work together and how their revolutionary cooperation is changing the connectivity and intelligence environment. Examining the merging of these cutting-edge technologies, it clarifies how the combination of 5G networks' high-speed, low-latency capabilities of IoT devices opens up previously unheard or unknown possibilities for improved data transfer and smooth device operation. The addition of Edge Computing with 5G and IoT strengthens the collaborative effort by providing decentralized data processing and real-time analytics, which in turn improves the responsiveness and effectiveness of IoT devices. It illustrates the wide range of applications across industries, from smart cities to healthcare, through illuminating case studies. This chapter addresses issues including security, privacy, and the requirement for defined protocols as it navigates the difficulties brought up by this combination. It acts as a thorough guide, shedding light on the three technologies' capacity to transform markets, spur invention, and open the door to a hyper connected future with unheard-of connections and intelligence break through.

Keywords: Information technology, internet, analytics.

Authors

Meenakshi Gupta
CSE Department
DPGITM Engineering College
Gurugram, India

Garima Choudhary
CSE Department
DPGITM Engineering College
Gurugram, India

I. INTRODUCTION

- 1. Introduction to IoT:** Everybody knows about the Internet. Its how people connect with each other every day. The IoT (Internet of Things) is an interrelated system that allows to connect with physical objects, devices, machines and everyday objects and allows those things to communicate with each other.

The Internet of Things (IoT) is the term used to describe the interaction and communication between billions of devices that generate and share data pertaining to real-world objects (i.e., things) [8].

The IoT allow object to be sensed and control remotely across a network, objects and computer system can integrate directly over the IoT. Each object connected on IoT has a unique identifier that lets other object on the network find and connect with it.

E.g., Your smart watch could share your vital sign with your doctor, parking meter could alert you when a space is free, or your air conditioner could time its cooling cycle for when utility rates are lowest.

- **History:** All though the term IoT was introduced in 1999. We can find its history all the way back to 1982. When four computer science engineering students at Carnegie Mellon connect their building coke machine to the internet. So, they could check from their desk whether it was stocked before they trekked down in the lobby.

From this humble beginning, a technology has risen that could completely reshape the society thinks about design and uses commercial and industrial devices.

Some call the Internet of Things (IoT) “**The next Industrial Revolution**”

- **Business Perspective:** The Internet of Things (IoT) promises to reform the way businesses provide value to their customers. It permits objects to be sensed and controlled remotely across an existing network infrastructure

By 2025, research indicate that number of IoT connected devices globally could exceed 30-40 billion. Since the expected population of 2025 is a little over 8 billion peoples. That’s 4 or 5 connections for every person on the planet.

Smart business leaders are prepared for this future. Most of them say they believe the IoT will have a major impact on the future of their company. It means they are planning to incorporate the IoT into their product and services to create smart, connected product. One prevailing technology that keeps an eye on the connected smart devices is the Internet of Things. The fourth industrial revolution is being enabled by the Internet of Things. It has had a remarkable effect on technological, social, economic, and human and machine life [1].

The possibilities range from completely revolutionizing the agriculture, manufacturing, energy and transportation industries to more humble but pervasive changes in the people's day to day life.

- **Application:** The properties of IoT, such as its ultra-large-scale network of things, device and network level heterogeneity, and the high volume of events it generates, will make it very difficult to create a variety of applications and services [9].
- Picture yourself in the morning, brushing your teeth while standing on your bathroom scale. Your toothbrush offers real time feedback on your brushing technique and your scale charts changes in your body temperature, fat percentage and BMI.
- In the kitchen, your refrigerator senses that you will be using the last of the egg for your omelet, so it adds a carton to home delivery grocery list. Meanwhile your car is not waiting idly in the garage. It is telling your home network that it low on gas and asking it to find the gas station with the best fuel prices and then chart the best route past that station for your drive to work through. The changes begin small, the IoT has the chance the reshape the way you live, saving time, increasing your productivity and providing you and others with valuable insight and information.
- With so many rising concerns about the changing climate it is becoming vital to know exactly what going on in the environment. Network connected devices and special sensors have begun to be used to monitor condition in the environment. Interconnected objects could also do things like measure climate conditions across the globe, and monitor drinking water quality, or soil conditions.
- They could even be used to track wildlife without intruding into their territories. Beside keeping the earth safer, the devices that surround you are beginning to collaborate, to keep you safer.
- Your car could suggest route changes to steer you around dangerous road conditions.
- Sensors in the oceans or along fault lines provide early alerts to tsunamis and earth quakes.
- Home surveillance systems provide owner with remote access to locks and alarm systems while they are at the office, or even on the other side of the world.
- Network capable devices may cost more than non-connected devices, but often offer greater potential savings overall.
- Home owner can enjoy savings by installing app that intelligently control their household energy consumption.
- Lighting system can turn themselves off as soon as you leave hoe and go on a moment before you enter.
- Homes or businesses with solar panels can feed the extra unused power back into the grid for further cost savings.
- Healthier lives for everyone could be the biggest benefit of the Internet of Things.
- Smartwatches could notify doctors of changes in vital signs, or recommend fitness routines that best fit your schedules, or summon help if they detect you have fallen or go into cardiac-arrest.
- The effect of the IoT on business and industry has been profound as well. For example, thanks of Iot connectivity, instead of selling aircraft engines, GE now sells the use of engines by the hour.

- Swiss escalator manufacturer Schindler integrates escalators and elevators across office campuses to keep them running optimally.
- Automation and robotics companies Rockwell and FANUC collaborate to seamlessly integrate production line and adjust flows for machinery problems.
- The IoT promises to change daily life in so many ways.
- **Challenges:** The centralized cloud computing architecture cannot effectively manage the new difficulties brought on by the burgeoning IoT, such as severe latency, capacity restrictions, resource-constrained devices, uninterrupted services with intermittent connectivity, and enhanced security [7].

For all the benefits the IoT will bring, it will have its share of challenges. With billions of objects collecting, sharing, and acting on an endless stream of information, urgent problem quickly arises, such as

- **Information Storage and Analysis:** Storage of data, finding ways to effectively analyze all the data, one of the biggest challenges of the IoT is that it involves such a tremendous of data as a person makes their way through their day, countless object connected by IoT tirelessly collect data on their likes, dislikes, habits and hardships. Businesses can tap into this slot of information, but they may be unable to invest in sufficient data storage to store it all.
- **Managing Data:** Another challenge for businesses is intelligently managing the data they do collect. For instance, social media companies have come under fire for not employing enough staff to monitor user contributions, leading to controversial content and behavior. To target the data that will best help them to make their customers happier and their bottom line stronger, businesses will need to invest in hiring experienced data analyst and acquiring advanced data mining tool to reap the benefits.
- **Security:** It seems like every headline these days about data security breach that has put the personal data of thousands into the hands of hackers. With the rush to jump on to the IoT bandwagon, many commonly used devices are rushed for delivery to the market without giving adequate attention to properly securing data, making those devices a weak link in network security systems. Hackers have built a network of thousands of such compromised devices, including such innocuous items as refrigerators and DVRs to launch their malicious attack from. And the greater the number of interconnections, the greater the security risk. If users are going to trust the IoT with more and more of their vital information, businesses will need to put greater care and thought into security design. Even the simplest of household devices will need to be designed with robust encryption, secure web interfaces, adequate software protection, and sufficient authorization.
- **Privacy and Confidentiality:** The IoT collects reams of information about you; where you are, where you are going, what you are buying and how you are feeling. Businesses use that information to improve their product and services. In return, customer expect businesses to keep that information private. If customer don't trust that the benefits of network-capable products are worth the risk of exposing private information, they won't invest in those products. Businesses need to balance the need to collect data with need to protect it. Only by demonstrating that they can balance those two needs responsibly will businesses start to build their customer's trust.

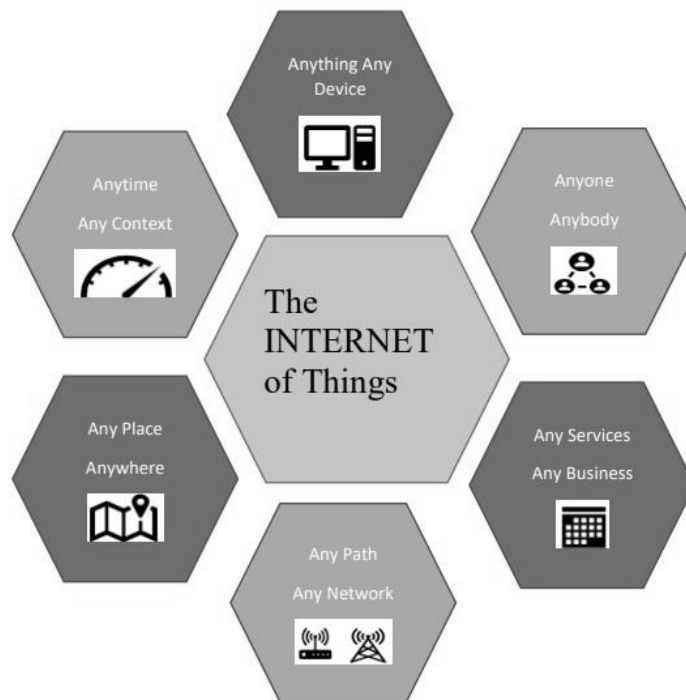


Figure 1 : Introduction to IoT

2. Introduction to 5G: In cellular networks, 5G is the fifth-generation wireless technology. After 4G (LTE) network, 5G is the latest progress in mobile communication standards. As compared to previous generations, 5G provides significantly faster speeds, less delays (low latency) which improve the performance of commercial applications. As we know peak speed of 4G is only 1 Gbps and 5G provides peak speed of 20 Gbps. 5G delivers next level connectivity from cloud to client, as it is software driven and uses cloud technology. This service is already available in some cities in numerous countries by 2022. To boost the flexibility of network resource allocation and the capacity of 5G networks based on network slicing, effective resource allocation strategies should be taken advantage of because of the rising huge wireless data traffic from various application scenarios [2].

New mobility management strategies are desperately needed to ensure seamless changeover in network-slicing-based 5G systems due to the variety of 5G application situations

- **Key characteristics of 5G**

- **Network Slicing:** - A promising technique for 5G networks is network slicing, which enables services that are specifically suited to consumers' QoS requirements [2]. To meet specific 5G application necessities, network slicing permits creation of virtual network partitions. It caters different use cases, ensuring optimum performance and quality of service by permitting tailored network configurations.
- **Minimum Latency:** - By decreasing the delay between the transmitting and receiving data, 5G attempts to attain the ultra-low latency. Expected low latency is around 1

millisecond, with this 5G enables the real time application like remote surgeries, self-directed vehicles and augmented reality practices.

- **High-Speed Connectivity:** - 5G has almost 20 Gbps data transfer speed that is extremely high. And this high speed allows faster download, faster streaming and faster real time communication.
- **Increased Bandwidth:** - Due to high-speed connectivity 5G has data transfer speed and improved network capacity. And for this it utilizes wide frequency bands because high frequencies band have higher frequency ranges such as mm Wave (millimeters waves). Higher frequency band means increased bandwidth.
- **Edge Computing:** - Edge computing means distributed computing technique. In edge computing data storage and data processing done at the edge of the network and it reduces the latency, enables faster response time for real time applications. Computing capabilities of edge computing technology are integrated with 5G networks.
- **Mass Device Connectivity:** - A huge number of linked devices can be supported at once by 5G networks. For the Internet of Things (IoT) to expand and allow for the continuous communication and interaction of billions of devices, this capacity is vital.
- **Enhanced Security:** - The advanced security features are used to protect against cyber threat by 5G networks. For creating a secure and trusted environment for transmission of data 5G uses different transmission methods such as encryption, decryption, authentication and network slicing techniques.
- **Enhanced Coverage:** - In comparison to prior generations, 5G network provides better coverage. Beamforming techniques and multiple-input, multiple-output (MIMO) technology can improve connection in distance places by minimising dead zones and enhancing signal transmission.
- **Enabling Advanced Application:** - All key features discussed above makes the way for advanced applications of 5G including driverless vehicles, smart cities, industrial automation, remote surgeries, virtual reality, and augmented reality experiences.

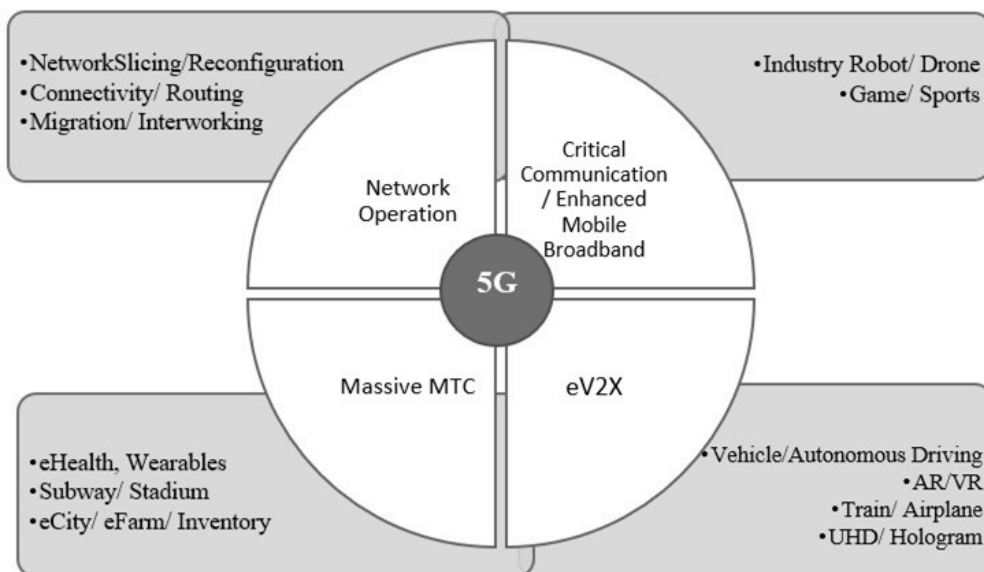


Figure 2 : 5G Characteristics

3. Introduction to Edge Computing: Edge computing is used by businesses to increase the responsiveness of their remote devices and to gain deeper, more timely insights from device data. Real-time computing is made possible by edge computing in places where it would not otherwise be conceivable, and it also lessens congestion at the networks and data centers which serve edging devices.

Edge computing is a novel computing paradigm that places computing and storage resources (such as cloudlets, mini data centers, fog nodes, etc.) closer to mobile devices or sensors [5].

In the absence of edge computing, the enormous amount of data created by edge devices would swamp the majority of present day's commercial networks, impeding all functionalities on a hampered network. Expenses for IT may soar. Customers who are not happy may go to a competitor. Valuable equipment can get hurt or just work less well. The safety of workers could be jeopardized in businesses that depend on sophisticated sensors to keep them secure, which is the most crucial concern.

For example

- a retail outlet 1,100 miles from the organisation's main data centre employs wireless point-of-sale equipment to process payments instantaneously.
- By monitoring the moisture of the soil level, an irrigation system in a far-off farm field changes the amount of water it consumes in real-time.
- AI and IoT sensors are used on an oil rig in the midst of the sea to promptly identify problems with devices before they get worse.

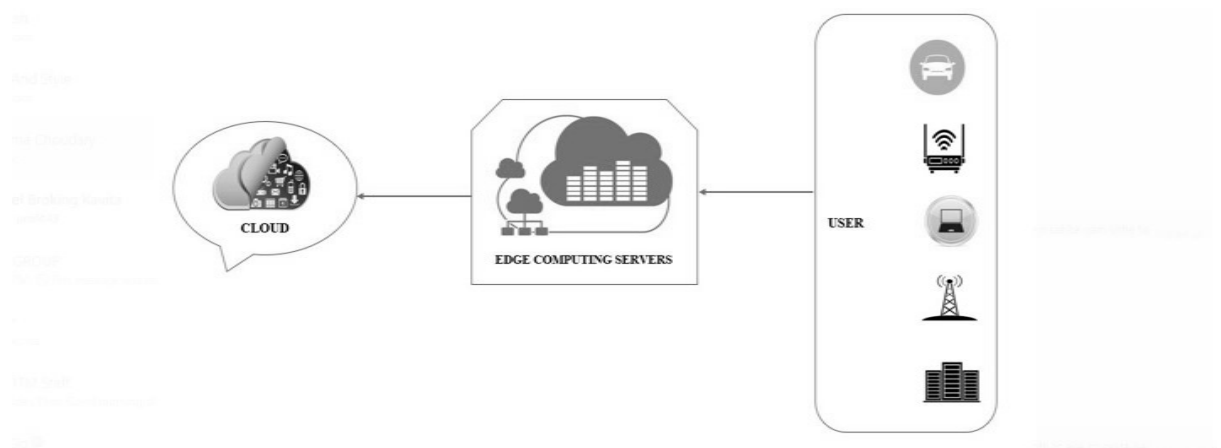


Figure 3: Introduction with Edge Computing

- **Advantages of Edge computing:** Without uploading to a cloud computing platform, the edge computing paradigm stores and processes data on edge devices. Edge computing benefits in the following areas are clear as a result of this feature [4]. The advantages of edge computing are numerous, ranging from security and productivity to workplace safety:

- **Increased Operation Efficiency:** Edge computing helps organizations by processing vast amounts of data fast at or close to the local locations where the data is being collected. This helps businesses streamline daily operations. This is more efficient than transmitting all the acquired data to a primary datacenter in a separate time zone, which would cause severe network delays and performance issues.
- **Rapid Response Time:** Edge computing allows businesses to handle data more rapidly and reliably, in real time or close to it, by avoiding centralized cloud and datacenter sites. If information were to be sent simultaneously from hundreds of sensors, cameras, or other smart devices to a central office, consider the data latency, network bottlenecks, and poor data quality that may result. In contrast, edge computing enables devices at or close to a network's edge to instantaneously notify essential personnel and equipment of mechanical problems, security risks, and other crucial situations so that immediate action can be done [3].
- **Increased Productivity of the Workforce:** Businesses may more rapidly provide employees with the information they need to fulfil their job responsibilities as effectively as possible thanks to edge computing. Edge computing also ensures that in automated and proactive maintenance-enhanced smart workplaces, the equipment that employees depend on runs without hiccups or easily avoidable mistakes.
- **Enhanced Workplace Security:** IoT sensors and edge computing can help keep people safe in workplaces where defective equipment or modifications to working circumstances might result in accidents or worse. For instance, predictive maintenance and real-time data analysis at or near the equipment site can assist boost worker safety and reduce negative effects on the environment on offshore oil rigs, oil pipelines, and other remote industrial use cases.
- **Ability to Function in Remote areas:** Edge computing facilitates the use of data gathered at remote locations with sporadic internet connectivity or constrained network bandwidth, such as a fishing vessel in the Bering Sea or a vineyard in the Italian countryside. Sensors are capable of continuously monitoring operational data, such as soil or water quality, and taking appropriate action as needed. Once internet access is established, the pertinent data can be sent to a centralized datacenter for processing and analysis.
- **Enhanced Security:** Businesses are very concerned about the security risk posed by integrating their network with thousands of internet-connected sensors and devices. By enabling businesses to process and store data locally, edge computing helps to reduce this risk. By reducing the amount of data sent over the network, this makes businesses less susceptible to security risks.
- **Cost Savings in IT:** Edge computing enables companies to save IT expenditures by analyzing data regionally instead of in the cloud. Edge computing decreases the communication costs by eliminating pointless data at or adjacent area where it is collected, in addition to reducing businesses' cloud processing and storage costs.
- **Data Sovereignty:** Organizations must follow local data privacy laws, such as the General Data Protection Regulation (GDPR) of the European Union, when collecting, processing, storing, and otherwise using consumer data. Adhering to data sovereignty standards can be challenging when moving data to the cloud or to a core datacenter across international boundaries, but edge computing enables organizations to guarantee that they are abiding by local data sovereignty rules by processing and storing data close to where it was collected.

- In order to meet the industry agility key requirements in connection, real time business, data optimisation, application intelligence, security and privacy, a near by open platform that integrates core capabilities such as networking, computing, storage and applications and offers edge intelligent services is needed [6].

II. IOT WITH 5G

A significant portion of the deployment of IoT devices is made possible by 5G networks. The administration and integration of IoT devices is made possible by 5G. To support the enormous number of connected devices, 5G delivers significant scalability and capacity enhancements in comparison to previous generations. Let's go through some of the main characteristics that make 5G capable of managing the higher device density

- **Minimum Latency:** The term “Latency” means delay between the transmission and reception of data. Response time of 5G is as low as few milliseconds so that 5G has ultra-minimum latency. For IoT applications, minimum latency is required and 5G networks fulfil this condition. To form efficient and responsive IoT systems, 5G allows instantaneous communication among devices.
- **Network Reliability:** 5G networks are more dependable than earlier generations. To guarantee a more dependable and steady network connection, they use cutting-edge error correction algorithms, redundancy systems, and strong signalling protocols. For mission-critical IoT applications like smart grid management, emergency response systems, and remote monitoring of crucial infrastructure, this stability is essential.
- **Enhanced transmission Data speeds:** 5G networks offer significantly higher data speeds than earlier cellular network generations. IoT devices may send and receive data more quickly thanks to the enhanced bandwidth. Less internal memory is needed by linked devices when cloud technology is used more frequently. As cloud computing may be used, it is not essential to install additional processors on the device. For applications that need real-time data processing, such driverless vehicles, industrial automation, and remote healthcare, this is essential.
- **Support for Edge Computing:** 5G networks make it easier to integrate edge computing with IoT devices. Edge computing reduces the amount of time data must travel between IoT devices and distant cloud servers by processing data closer to the source. 5G networks reduce latency and improve real-time decision-making capabilities for IoT applications by enabling edge computing.
- **Mass Device Connectivity:** The influence of 5G networks on IOT is obvious from the rise in the number of devices utilizing the network. IoT devices can number somewhere between a few hundred and billions, and 5G networks use cutting-edge strategies like network slicing and dynamic resource allocation to effectively manage this enormous size. It is possible to install IoT systems on a broad scale without running into congestion or performance deterioration because to 5G networks' capacity to accommodate a high density of devices.
- **Longer Battery Life:** Energy-saving measures built into 5G networks enable IoT devices' batteries last as long as possible. IoT devices frequently use finite power sources, therefore they must preserve energy to maintain functioning for an extended period of time. With 5G, devices can connect quickly and effectively, transmit data in bursts that are shorter, and intelligently use sleep modes to conserve battery life.

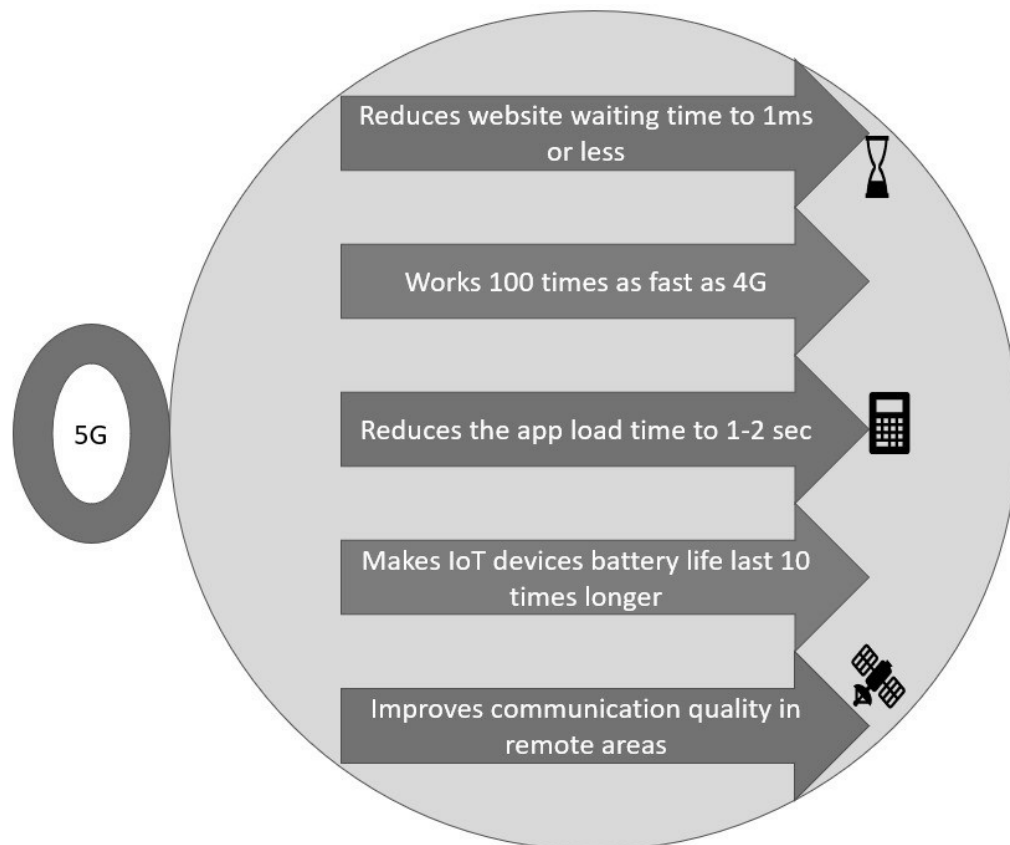


Figure 4: IoT with 5G

- **Application for IoT using 5G:** Advanced Internet of Things (IoT) applications are made possible by 5G networks, especially in areas like industrial automation, smart cities, and driverless vehicles (autonomous car). Here is how 5G makes these applications possible:

Industrial Automation: To optimize manufacturing processes, increase productivity, and enable predictive maintenance, industrial automation primarily relies on IoT technologies. The advantages of 5G networks for industrial automation are as follows:

- **Ultra-Reliable Communication:** Critical industrial applications require consistent and predictable connection, which is provided by 5G's ultra-reliable and low-latency communication (URLLC) capabilities. This is crucial for tasks like robotic control systems and real-time monitoring that call for exact synchronization, great responsiveness, and low error rates.
- **Network Slicing and Quality of Service (QoS):** With 5G's network slicing and QoS features, industrial automation applications can have dedicated network slices that ensure a particular level of performance, latency, and reliability. As a result, mission-critical operations can run as efficiently as possible with the least amount of interruption.

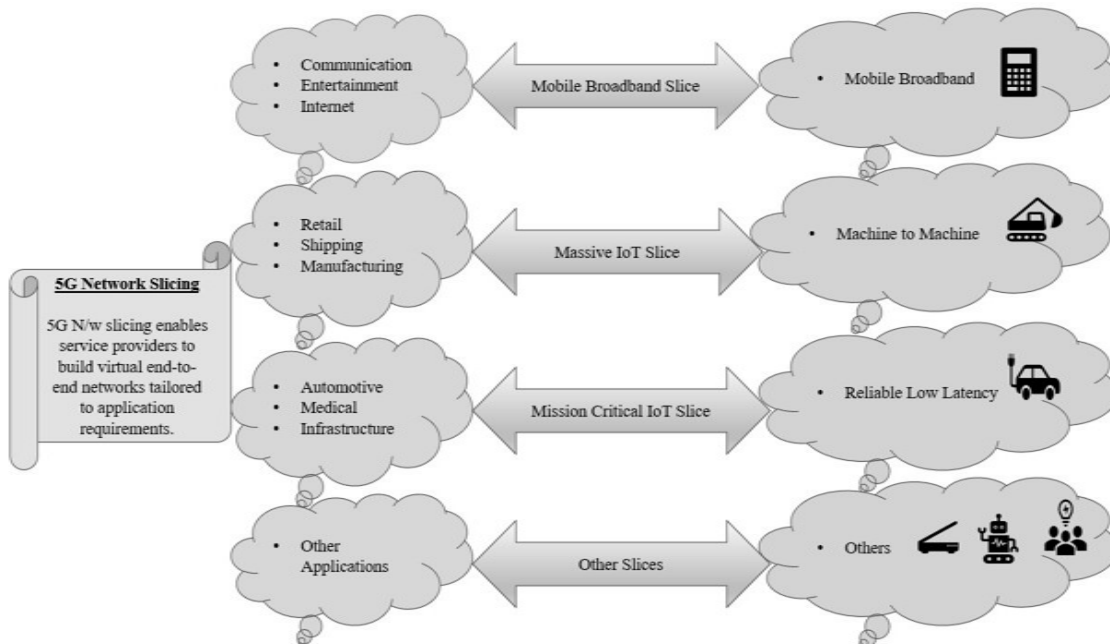


Figure 5: Network Slicing

- **Massive Machine-Type Communications (mMTC):** A 5G feature called mMTC offers huge connectivity for a significant number of IoT devices in an industrial setting. This makes it possible for sensors, actuators, and other IoT devices to seamlessly integrate into the automation ecosystem, providing thorough monitoring and control of industrial operations.

Smart Cities: Smart cities use IoT technologies to enhance public services, optimize urban infrastructure, and enhance the overall quality of life for residents. The following benefits of 5G networks are available for smart city applications:

- **Massive Device Connectivity:** Compared to earlier generations, 5G allows a much higher density of connected devices per square meter. This makes it possible for a wide range of IoT devices, such as smart sensors, security cameras, and environmental monitoring systems, to communicate seamlessly throughout the city.
- **Edge Computing:** 5G networks make it possible to use edge computing, bringing computational power closer to the data source. As a result, there is less latency and dependency on centralized cloud infrastructure because smart city applications can process and analyse data locally. Critical services like traffic control, emergency response systems, and public safety apps may now make decisions in real time and respond more quickly thanks to edge computing.
- **Low Power Consumption:** 5G introduces technologies like Narrowband IoT (NB-IoT) and LTE-M, which were created expressly for low-power IoT devices. These innovations enable smart city equipment to run for longer periods of time on battery power, lowering maintenance requirements and overall energy usage.

Driverless Vehicle (Autonomous Car): For real-time communication and decision-making, autonomous cars need dependable and low-latency connectivity. 5G networks offer the following major benefits:

- **Minimum Latency:** 5G's minimum latency capabilities allow autonomous vehicles and their surroundings to communicate almost instantly. This improves safety by enabling prompt responses to urgent directives and enabling vehicles to respond in real-time to shifting road conditions.
- **Network Slicing:** The network slicing feature of 5G enables the development of specialized virtual networks suited to particular needs. In order to ensure dependable and ongoing communication even in busy network situations, this enables autonomous vehicles to have their own dedicated network slice.
- **Increased Bandwidth:** Using a variety of sensors, cameras, and communication systems, autonomous cars produce a significant amount of data. Increased bandwidth provided by 5G networks enables the seamless transmission of significant amounts of data for perception, decision-making, and coordination between infrastructure and vehicles.

III. IOT WITH EDGE COMPUTING

The Internet of Things gains a lot of advantages from edge computing. Reduced latency, increased availability and resilience, cost savings, and local data storage (to help with regulatory compliance) are a few examples. These advantages are used to determine the exact location of the edge. Let's now examine more closely how edge computing advantages manifest themselves in actual IoT use cases.

1. **Enhanced availability and resilience:** To guarantee security and service continuity, critical infrastructure demands the highest level of availability and resilience. Think about a technique to find gas leaks in refineries. It must be capable of working without an Internet connection. A problem arises if there is a leak and the system goes offline. There must be edge computing. The system itself may have the advantage in this situation.

Even though it's not a use case that puts lives in danger, retail operations can profit from the availability offered by edge computing. Retailers desire 100% availability of their Point of Sale (PoS) systems to serve customers. However, several retail stores are situated in outlying areas with erratic WAN connections. PoS systems being moved to edge computing.

2. **Reduced latency:** Many applications have stringent latency requirements, but for safety and security applications, latency can literally mean the difference between life and death. Think about an autonomous vehicle that applies the brakes or a sign that alerts drivers to impending dangers on the roadside. Lives may be in risk by the time data is transported to the cloud for analysis, when a result is returned to the car or sign. But let's do some fun math with some numbers.
3. **Reduced Cost & Increased Bandwidth;** Although practically limitless, bandwidth has a price. By processing data before it travels across the WAN, edge computing enables businesses to save bandwidth expenditures. While this benefit can be applied to any use case, video surveillance and preventive maintenance are two use cases where it is particularly clear. For instance, a single HD video camera placed in a city may produce 1,296GB every month. It becomes quite expensive to stream that data through LTE. These costs are greatly decreased by using edge compute to pre-aggregate the data.

Manufacturers employ edge computing for remote machinery preventive maintenance. Temperatures and vibrations are monitored using sensors. The accuracy of this data is crucial because even the smallest change can point to an issue. To make sure problems are discovered.

- 4. Obey governmental regulations:** Data retention and privacy rules are being implemented by nations more frequently. General Data Protection Regulation (GDPR), which is enacted by the European Union, provides a good illustration. The GDPR imposes obligations on organizations, including the need to report personal data leaks, and every entity that has data belonging to an EU individual must comply. These firms can comply with GDPR with the assistance of edge computing. A smart city may, for instance, assess the surveillance footage at the edge and only backhaul the meta data rather than keeping and backhauling the video.

The National Hydrometric Program under the Canada's Water Act is another edge computing use case that helps with regulatory compliance. Nationwide, around 3,000 measurement stations have been put into place as part of the program. It is necessary to explain any missing data. But keeping data at the edge ensures data retention.

Edge computing creates new opportunities for Internet of Things use cases by lowering latency and costs, enhancing resilience and availability, and maintaining local data. These are simply the start of many more. It will be interesting to watch where edge computing will next appear.

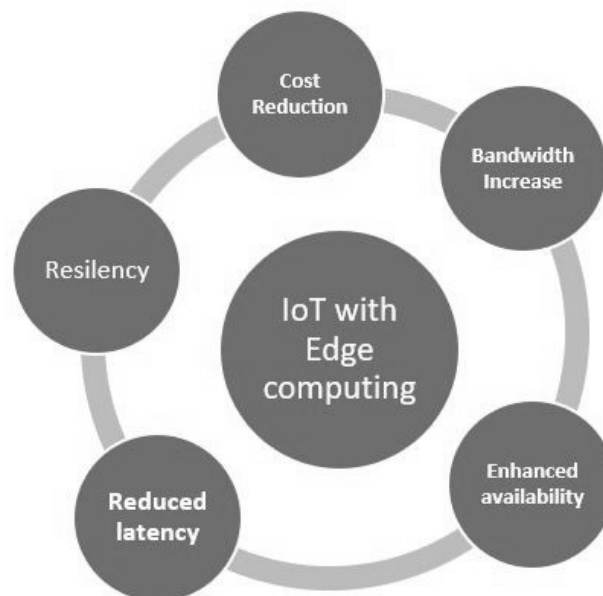


Figure 6: IoT with Edge Computing

- **Security and Privacy Considerations:** Addressing the security challenges brought on by the proliferation of IoT devices in a 5G environment. Security will suffer significantly as a result of these new networked ecosystems. The main obstacle will be the attack surface's abrupt, exponential growth brought on by the IoT's rapid growth and edge computing. This will be soon followed by the fact that these devices won't always be linked to a central network in a conventional hub-and-spoke setup. Any device might become the weakest link in the security chain and put the entire organization at risk because there are literally billions of IoT devices connected across a meshed edge environment. Some major changes in the way we see networking and security will be necessary to meet this issue.
- **Access and Control:** Edge-to-edge security will be required, starting at the IoT edge and extending through the enterprise network core, branch offices, and several public clouds. This requires the identification, criticality grading, and status confirmation of every component of the enterprise ecosystem. A verification, validation, and authentication process will subsequently be required for all requests to access network resources.
- **Network Segmentation:** Security must also support edge-to-edge hybrid systems that are elastic and combine tried-and-true conventional methods with novel ideas. Old tactics may not be the most effective in a 5G environment, even if network segmentation is a tried-and-true method for limiting cybersecurity risks and safeguarding sensitive resources. Navigating local and remote resources that blend segments over which companies may or may not have control will require new segmentation strategies. When implementing 5G networks and public cloud services, IT teams will need to consider how to handle the complexity of many co-managed systems.
- **Tool-to-tool compatibility with security:** Along with the use of vendor-neutral APIs, agnostic management tools that can be centrally controlled to observe security events and orchestrate security policies, the creation of new open 5G security standards, and interoperability across various security tools are further requirements.
- **Making Use of a New Security Architecture:** Deep integration of security systems will be necessary for sharing threat intelligence, correlating event data, and facilitating automated incident response. A thorough, fabric-based security architecture will need to be created and implemented in order to achieve this. The key to expediting decision-making and bridging the gap between detection and mitigation will be machine learning, artificial intelligence, and automation.
- These are only a few of the security repercussions of 5G network adoption and deployment. The effects of this new networking and computer era are only now beginning, though. In terms of security, the following situations must be considered:
 - Security must be able to travel between and across various network ecosystems without losing sight of workflows or sacrificing security functionality in order to support distributed network applications that are optimized for the cloud.
 - In order to guarantee that constant innovation incorporates persistent protection, automated network application lifecycle management will necessitate security systems that are not only highly performant but also extremely adaptable. To ensure that security is integrated directly into the development strategy, it will also be necessary for enterprises to switch from a DevOps paradigm to a DevSecOps approach.

- Massive volumes of new data, the majority of which will be encrypted, will be produced by the digital transformation. More than 70% of network traffic at the moment is encrypted data. As more open network environments adopt encryption to secure data transmission, that percentage will only increase. IoT and other edge devices will need to have high-performance security tools installed in order to be able to quickly and thoroughly evaluate encrypted traffic.
- Organizations will be able to more effectively use resources going through huge data environments thanks to new tactics like network slicing. To protect crucial resources while isolating them from open and less secure environments, segmentation and edge-based micro segmentation will also be necessary.

IV. SECURITY MEASURES

Strong security measures are essential for safeguarding private information and securing sensitive data in IoT devices, especially in the context of 5G networks. As 5G technology becomes more prevalent, there are many potentials to connect more devices, provide faster communication, and support cutting-edge applications. However, because of the expanded scope, complexity, and interconnectedness of IoT devices, it also poses new security challenges. IoT device security in the context of 5G is critical for the following reasons:

- 1. Data Protection:** IoT devices produce and send a lot of delicate data. These data might contain contact information, geographic information, health information, and more. To prevent this data from being intercepted, altered, or accessed by unauthorized parties, strong security measures are needed. To protect data privacy, it is important to implement strong encryption, secure protocols, and access controls.
- 2. Protection Against DDoS Attacks:** As 5G networks make communication faster and more effective, IoT devices are more appealing targets for Distributed Denial of Service (DDoS) attacks. Strong security measures, such traffic monitoring, anomaly detection, and network segmentation, aid in the identification and mitigation of DDoS attacks, guaranteeing the availability and dependability of IoT devices and services.
- 3. Enhanced Connectivity and Scale:** The significant increase in connected devices made possible by 5G creates a huge attack surface for potential cyber threats. To protect these devices from unwanted access, data breaches, and harmful activity, strong security measures are required. To guarantee the privacy, accuracy, and availability of data, IoT devices must be built with secure communication protocols, authentication techniques, and encryption.
- 4. Reducing Device Vulnerabilities:** Because IoT devices frequently lack sufficient resources, it might be difficult to put effective security controls in place on the actual hardware. The device, network, and application layers are just a few of the places where security controls should be put in place. This multi-layered strategy aids in the detection and mitigation of vulnerabilities, preventing hacked devices or networks from causing significant security breaches.

5. **Secure Device Onboarding:** In order to deploy IoT devices on a 5G network, secure device onboarding practices are needed. Before allowing devices access to the network, this entails confirming the authenticity and integrity of the devices. In order to create trust between the devices and the network and stop unauthorized or malicious devices from getting access, robust security methods including secure boot, secure firmware updates, and digital certificates are used.

6. **Compliance and Regulations:** Businesses using IoT devices in 5G networks must abide by laws governing data security and privacy, including GDPR, HIPAA, and standards particular to the sector. Organizations can comply with these regulatory standards while avoiding legal repercussions and upholding their stakeholders' and consumers' trust.

REFERENCES

- [1] Sharma, Neha, Madhavi Shamkuwar, and Inderjit Singh. "The history, present and future with IoT." *Internet of things and big data analytics for smart generation* (2019): 27-51.
- [2] H. Zhang, N. Liu, X. Chu, K. Long, A. -H. Aghvami and V. C. M. Leung, "Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges," in *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138-145, Aug. 2017, doi: 10.1109/MCOM.2017.1600940.
- [3] www.azure.microsoft.com
- [4] K. Cao, Y. Liu, G. Meng and Q. Sun, "An Overview on Edge Computing Research," in *IEEE Access*, vol. 8, pp. 85714-85728, 2020, doi: 10.1109/ACCESS.2020.2991734.
- [5] M. Satyanarayana, "The Emergence of Edge Computing," in *Computer*, vol. 50, no. 1, pp. 30-39, Jan. 2017, doi: 10.1109/MC.2017.9.
- [6] X. Hong and Y. Wang, "Edge computing technology: Development and countermeasures", *Chin. J. Eng. Sci.*, vol. 20, no. 2, pp. 20, 2018.
- [7] Chiang, Mung, and Tao Zhang. "Fog and IoT: An overview of research opportunities." *IEEE Internet of things journal* 3.6 (2016): 854-864.
- [8] Ganz, Frieder, et al. "A practical evaluation of information processing and abstraction techniques for the internet of things." *IEEE Internet of Things journal* 2.4 (2015): 340-354.
- [9] Razzaque, Mohammad Abdur, et al. "Middleware for internet of things: a survey." *IEEE Internet of things journal* 3.1 (2015): 70-95.