Research on Cybersecurity Threats and Solutions in Edge Computing

MINT-709

Capstone Project Report

Presented by

Sumair Sufiyan Mohammed

University of Alberta

Master of Science in Internetworking

Department of Electrical and Computer Engineering

Supervisor

Sandeep Kaur

ABSTRACT

In recent years, edge computing has been accelerated greatly by the proliferation of IoT and smart mobile devices. While edge computing has been of immense help to mobile devices in their quest to complete complex tasks, its rapid growth has led to a widespread disregard for security risks in edge computing platforms and the apps they allow. This research is about attacks on cybersecurity in edge computing and how to stop them. The study looks at all the research on the subject and analyses the different types of security threats that can affect edge computing, such as data interception, device tampering, and malware attacks.

DDoS assaults, to be more exact, are the centre of our attention because they are responsible for thirty percent of all edge computing attacks that have been recently reported by Statista. Edge computing, IoT, 5G and Cloud Computing are the key drivers of the digital transformation that is taking place across industries. However, as the use of these technologies becomes more widespread, so does the number and complexity of cybersecurity threats. This research investigates the cybersecurity attacks and solutions in edge computing, IoT, and cloud computing, examining the interplay between these technologies and their associated security risks.

The report emphasises the need for defence-in-depth to solve edge computing's broad and complex security issues. The report also emphasises the necessity for industry professionals, governments, and researchers to collaborate on cybersecurity strategies and best practises that can adapt to the ever-changing cybersecurity scene. This research can help companies secure and protect their edge computing platforms.

ACKNOWLEDGEMENT

I am pleased to express my gratitude to my mentor, **Ms. Sandeep Kaur**, who guided me throughout the project and provided invaluable motivation and suggestions to expand my knowledge base. In addition, she offered insight and freedom to work on my project while ensuring that I stayed on track and did not stray from my project's core.

I would also like to express my sincere gratitude to my professors, **Dr. Mike McGregor** and **Mr. Shahnawaz Mir,** for providing me with assistance and such a great opportunity.

Last but not least, I would like to express my gratitude to my classmates, professors, and the University of Alberta for assisting and supporting me in achieving this goal whenever feasible.

Table of

Contents

Table of Figures

1 Evolution of Wireless Mobile Communication

In 1895, Radiotelegraphy was developed for wireless communication by transmitting Morse code through EM waves. Electronic magnetic wave (EMW) transmission and reception are employed in modern wireless communication. Transmission via radio waves was followed by cellular telephone and data networks. The development of wireless communication has progressed at a tremendous speed.

Every ten years, the radio access technology for mobile communications has developed into a new generation of technology. In tandem with technical advancement, services also have advanced. In the years between the first generation (1G) and the second generation (2G), the services mainly consisted of voice calls, but text messaging eventually became mainstream. The third generation (3G) technology enables the use of data communication services like the transmission of multimedia data such as images, music, and video by anyone. LTE (Long Term Evolution) technology enabled high-data-rate connection exceeding 100Mbps in the fourth generation (4G), leading to the explosion in the popularity of smartphones and the creation of several multimedia communication services. The 4G technology has continued to advance in the form of LTE-Advanced (VOLTE-voice over LTE) and has now reached a maximum data transfer rate of over 1 Gbps. Further advancements in technology have made the fifth generation (5G) a reality[1].

The evolution of mobile networks from the first generation (1G) to the fifth generation (5G) has enhanced the quality of interactions between people and their various forms of communication. In 2020, the infrastructure for the fifth generation of wireless communications, or 5G, became live in order to meet the present and future demands of wireless devices and networks. Trends in cellular technology over time are depicted in figure 1.

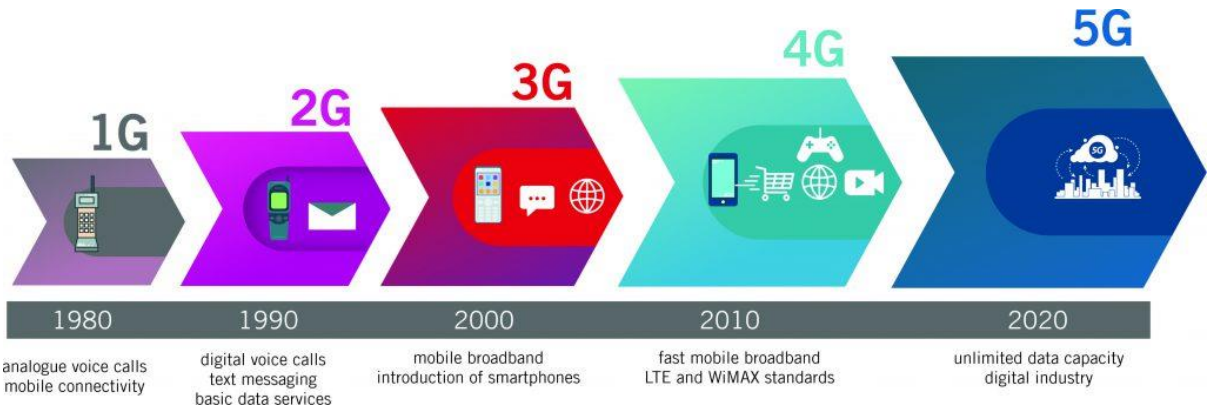

Figure 1 Trends in cellular technology [1]

1.1 First Generation (1G) Cellular Technology:

First-generation (1G) mobile cellular technology, known as NMT (Nordic Mobile Telephone) and introduced in the 1980s, provides voice services. Beginning in the 1980s, 1G was offered as an analog system with a circuit-switched network. The FDMA technology was utilized exclusively for voice operations on the 1G mobile system (Frequency Division Multiple Access). Operating frequencies were between 800 and 900 MHz, with a maximum channel capacity of 30 kHz. It had limited capacity, poor reception, poor battery performance, interference from ambient noise, etc. The telephone and fixed transceivers are examples of 1G devices. These devices utilised a single cell, and if they moved into multiple cells, the call would be dropped.

The Standard technologies that are used in 1G are Nordic Mobile Telephony (NMT), Advance Mobile Phone System (AMPS), Total Access Communication System (TACS), Push-to-talk (PTT), Improved Mobile telephone Services (IMTS), Mobile Telephone Systems (MTS).

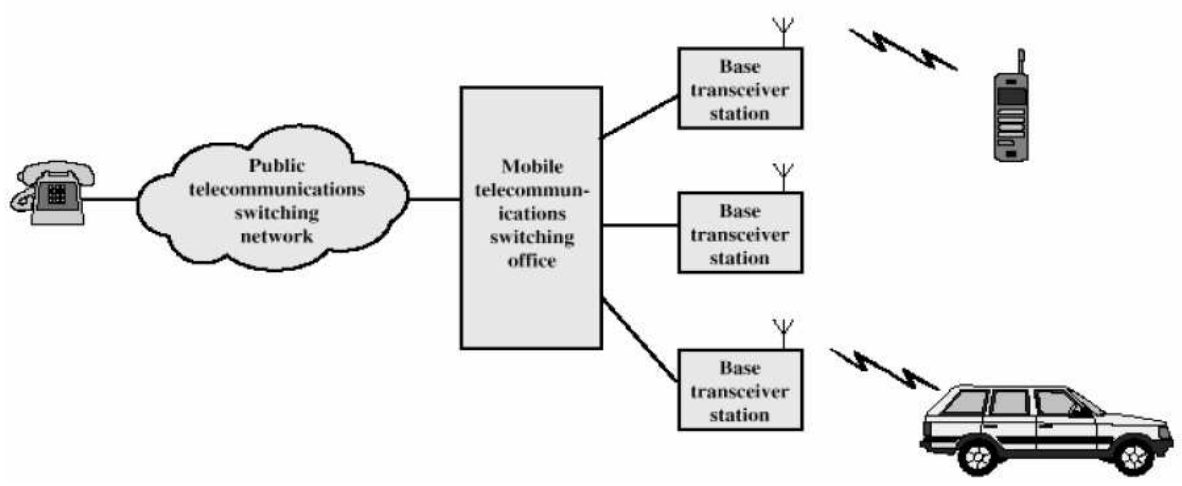

Figure 2 Basic AMPS architecture [2]

1.1.1 Attributes:

1. Can be used in Analog systems
2. Only voice calls were available.
3. Lower performance because of FDMA multiplexing
4. allowed for wireless communication to thrive.

1.1.2 Disadvantages:

1. Low quality of voice-over calls
2. Very bad handoffs
3. Limited range for bandwidth
4. The security is very weak

1.2 Second Generation (2G) Cellular Technology:

The launch of 2G cellular technology in the 1990s, which was based on digital system technology, was a major step forward in the development of wireless cellular technology. While 2G was still in its infancy, certain commercial data services were made available. As the first 2G network, GSM combined voice and data transmissions. In 2G, circuit-switched

networks are used for voice transmission and packet networks for data transmission and reception. In 2G, noise interference and voice quality were also enhanced. Digital encryption was originally deployed for data transmission security in 2G. The ability to send and receive text messages is provided by 2G. (Short Message Service).

The next generation of GSM technology is known as GPRS, which is often referred to as 2.5G. In this technology, the data transfer rate was increased to up to 150 Kbps. Following the launch of 2.5G, a new technology known as EDGE was deployed as part of the 2G network (Enhanced Data rate for GSM Evolution). In most cases, it has a maximum data rate of 384 Kbps and a GPRS of 2.75G, which is an upgrade over the previous version. For more efficient bandwidth/spectrum allocation, 2G systems utilised several access techniques such as a fusion of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA).

Figure 3 Different generations of 2G

1.2.1 Attributes:

1. Services like email and SMS were started.
2. Transmission rate is high compared to 1G

1.2.2 Disadvantages:

1. Problem with signals in densely populated areas.
2. Video transmission was not possible

1.3 Third Generation (3G) Cellular Technology:

Improved voice services, data throughput, good Quality of Service (QoS), and data security are hallmarks of third-generation cellular standards. In 2000, the International Telecommunications Union (ITU) unveiled a standard for third-generation mobile networks called IMT-2000. 3G has successfully reached data rates of 144 Kbps for mobile users, 384 Kbps for pedestrian users, and 2 Mbps for interior users [3].

All speech and data transmissions in 3G networks outside the air interface are handled by packet switching. Digital broadband, high-speed internet, and high QoS for better speech quality over the air interface are some of 3G's most distinguishing features. These are made possible by the network's equipment design, which addresses the noise interference problem that crippled its 2G predecessor. In 3G mobile cellular technology, the integrity of digital data and data security is improved. With broadband internet service, data speed went from 144 Kbps to 2Mbps, which is a huge jump. Services like voice, SMS, MMS, video, high-speed data, and video conferencing were put in place in the best path.

Two important types of 3G technology are 3.5G (HSDPA), which increases the speed of downlink data transmission from 8Mbps to 10Mbps, and 3.75G (HSUPA), which increases the uplink speed to 5.8 Mbps while decreasing the time it takes for the uplink and downlink to connect.

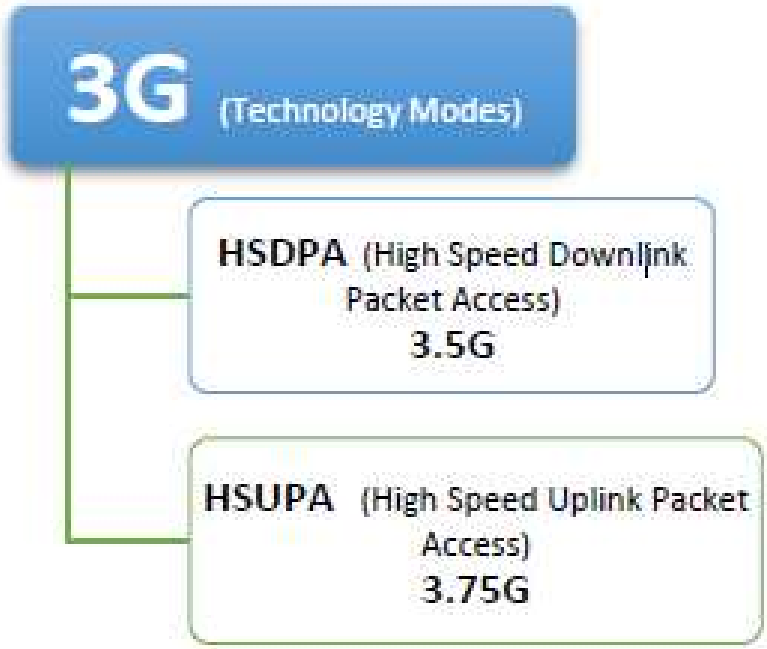

Figure 4 Different generations of 3G

1.4 Fourth Generation (4G) Cellular Technology:

The growing demand for a greater data rate for Internet access via mobile phones accelerated the development of the fourth generation of the cellular network to facilitate the transmission and broadcasting of broadband data for a large number of users. With 4G, we can send data as quickly as with earlier generations. Sending large quantities of data from a computer to a wireless device is now a simple process. Email, messages, and contacts are simply synchronizing and empowering users. 4G has increased bandwidth, a fast data rate, as well as seamless and quicker handoff, etc.

1.5 Fifth Generation (5G) Cellular Technology:

5G is a new technology that has piqued the interest of the research and development industry and will change the way users see slow wireless cellular technology. 5G cellular technology stipulates immediately that it must supply at least 1.0 Gbps to support virtual reality

environments with ultra-HD audio/video applications and 10 Gbps to support mobile cloud services.

As a uniform air interface, this technology has successfully provided end-to-end communication between everyday items such as smartphones, refrigerators, LED lights, cars, and metres. To put it another way, the launch of 5G will enable widespread, instantaneous access to anyone and everything, everywhere in the world.

To standardize 5G, two elite stakeholders collaborated. The International Telecommunication Union (ITU) Radiocommunication Sector was the first to propose specifications for 5G. It prompted the development of 3G (International Mobile Telecommunications, or IMT) in 2000 and 4G (IMT-Advanced) in 2008. As a result of these needs, 3GPP (3rd Generation Partnership Project), a coalition of key operators and communications companies, is currently playing a vital role in defining 5G technical specifications. The requirement for higher data rates and more efficiency is the primary force behind this progression from the first to the fifth generation. Technical requirements for IMT2020 and IMT advanced are summarised in the following figure.

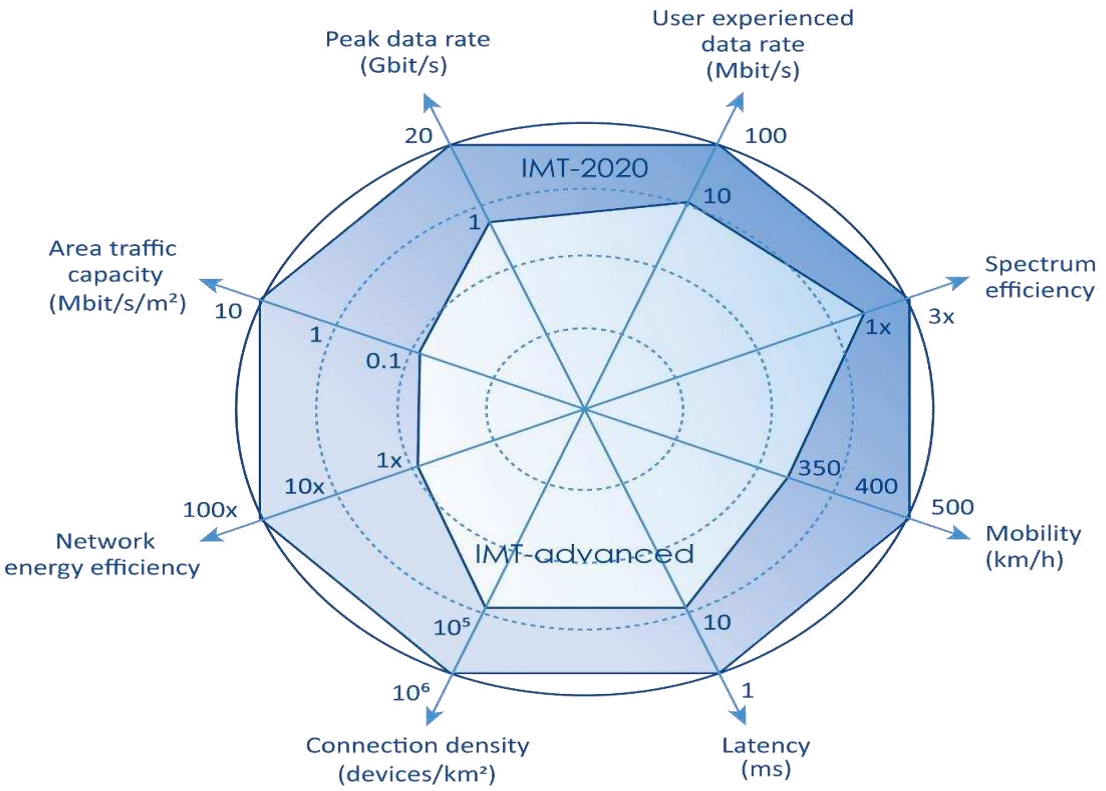

Figure 5 Comparison of key capabilities of IMT-Advanced (4th generation) with IMT-2020 (5th generation) [4]

1.5.1 5G Usage Scenarios:

The main usage of 5G case scenarios are eMBB, mMTC, URLLC.

- **Enhanced Mobile Broadband (eMBB)** to accommodate vastly greater data rates, high user density, and very high traffic capacity for hotspot scenarios, as well as flawless coverage and high mobility scenarios with even higher usage data rates.It is used mainly in VRs, ARs, Gaming and more
- **Massive Machine-type Communications (mMTC)** for the Internet of Things require low power consumption and low data rates for a vast number of linked devices. It gives longer battery life for IOT devices and mainly used in agriculture, wearables and inventory control technologies.

- **Ultra-reliable and Low Latency Communications (URLLC)** to cater for safety-critical and mission critical applications It is mainly used in industrial control, self-driving vehicles and health industry.

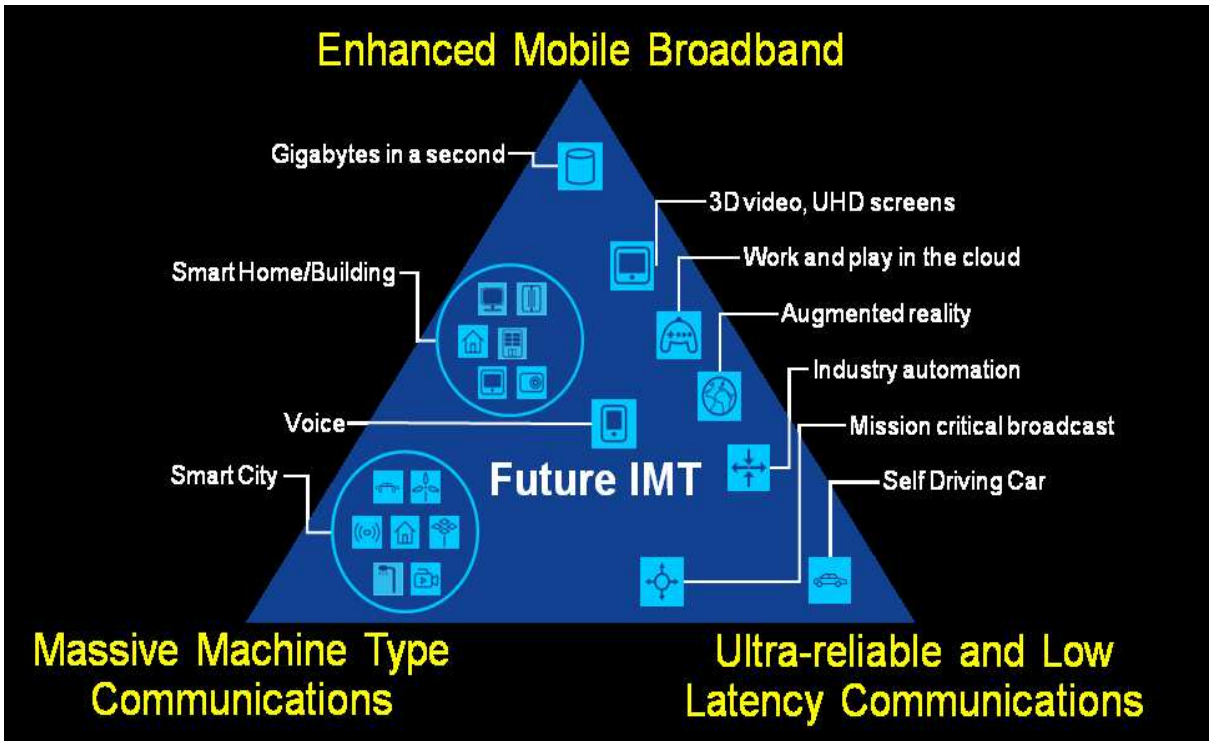

Figure 6 5G usage scenarios [4]

1.5.2 Architecture of 5G:

The fundamental objective of previous generations of mobile networks was to provide users with rapid and dependable mobile data services. 5G has expanded this capability to provide a broad range of wireless services supplied to the end user via numerous access platforms and multi-layer networks. Using a dynamic, unified, and adaptable architecture of cutting-edge technology, 5G can facilitate various uses. With 5G's more innovative architecture, Radio Access Networks (RANs) are no longer limited by their distance from the base station or the complexity of their supporting infrastructure. With the introduction of new interfaces, 5G paves the way toward a more disaggregated, adaptable, and virtual RAN that can accommodate growing data demands.

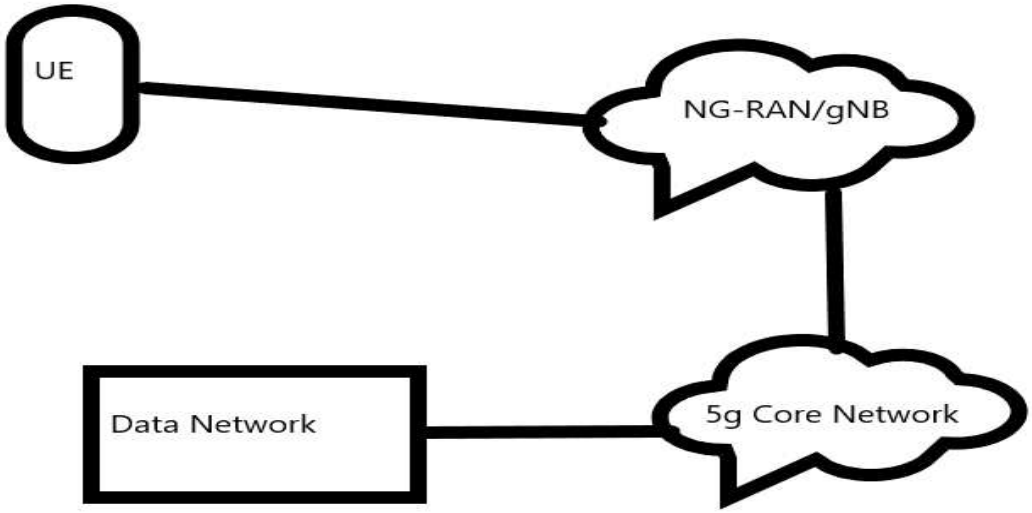

Figure 7 General Architecture of 5G

1.5.2.1 Components of Architecture:

- User Equipment (UE)
- Next generation- Radio access Network (NG-RAN)
- 5G base station is referred as gNB
- 5g core network contains of the IP architecture
- Data network is responsible for delivering higher data rates,

1.5.3 5G core Architecture:

The 5G core network architecture is crucial to the new 5G design and supports the increasing throughput demand that 5G must accommodate. According to 3GPP's specifications, the new 5G core is built on a cloud-aligned, service-based architecture (SBA) that handles everything from authentication and security to session management and end-device traffic aggregation. The 5G core emphasises NFV by deploying virtualized software functions via the MEC infrastructure, which is key to the 5G architectural concepts.

Each network function (NF) in this new architecture offers one or more services to other NFs via Application Programming Interfaces (API). Each NF comprises a collection of microservices, and small bits of software code. Some microservices can even be reused for many NFs, making implementation more efficient and enabling independent life-cycle management – allowing updates and new functionality to be delivered without influence on running services. Some of the network functions are policy control function, application function, session management function, authentication server function, network exposure function, NF repository function, network slice selection function. Network functions are depicted in the below 5g core architecture.

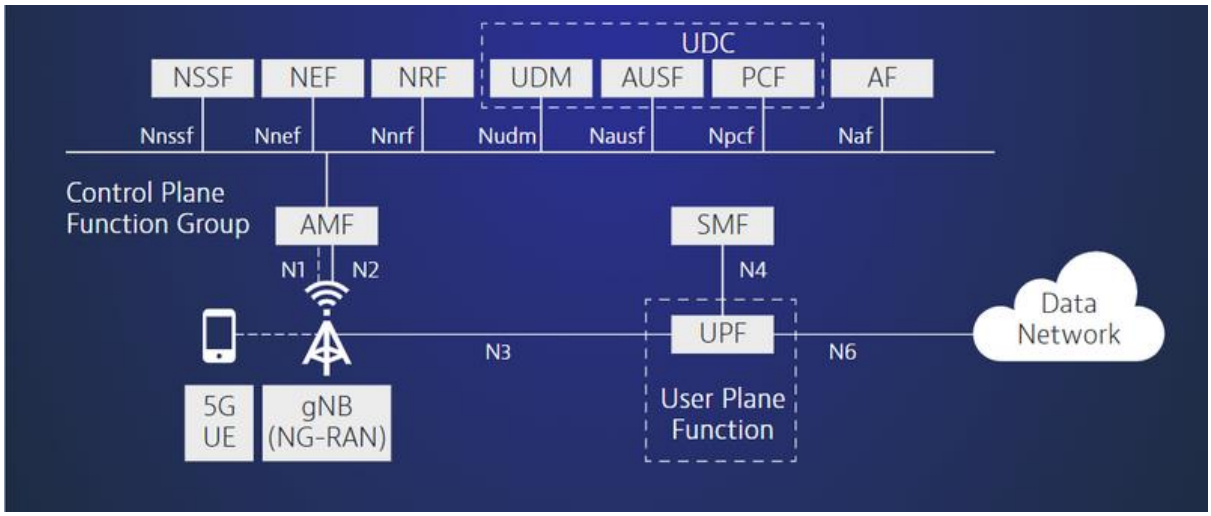

Figure 8 5G core Architecture [5]

5G architecture gives two modes of deployment Non-Standalone (NSA) mode and Stand Alone (SA) mode. Both NSA and SA utilise the 5G New Radio (5G NR) interface, allowing them to provide features and capabilities based on the 3rd Generation Partnership Project's standards (3GPP). 5G New Radio (NR) facilitates a transition from 4G LTE to 5G, which is one of its most important aspects.

1.5.4 Non-standalone Mode:

NSA is a 5G radio access network (RAN) that manages control plane tasks and operates on a legacy 4G LTE core known as Evolved Packet Core (EPC). The NSA has both a 4G and a 5G base station, however the 4G base station has priority. Because the NR control plane is anchored to the EPC, the primary 4G base station receives radio frequency signals. However, NSA 5G cannot provide certain functionalities that a pure, unrestricted SA 5G network can. For instance, the NSA does not enable the reduced latency which is one of the most attractive features of 5G. An additional downside of the NSA is that it requires more energy to power 5G networks using 4G infrastructure. The NSA architecture is appealing to service providers and commercial mobile network operators because it requires low or no EPC modifications. Benefits of NSA are reduced costs, easy deployment, fast rollout and it will also make easy to implement SA 5G.

1.5.5 Standalone Mode:

Cloud-native 5G cores and a 5G radio access network (RAN) are characteristics of SA 5G networks, while NSA networks rely on a 4G core. The 5G cores in SA networks allow for crucial 5G features like decreased latency, increased network performance, reduced power consumption and centralised control of network management. The only reason NSA 5G can deliver better mobile broadband is that its 4G core can be expanded to support the specification. SA can allow all the capabilities because its 5G core is more robust and adaptable.

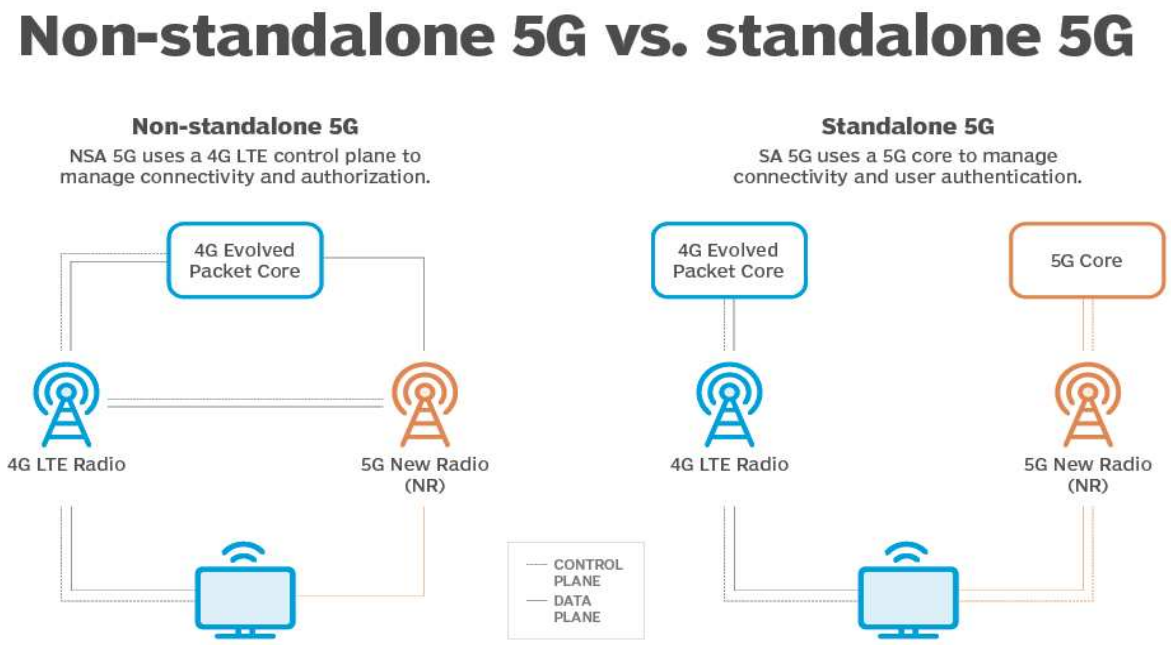

Figure 9 Comparison between NSA and SA mode [4]

1.6 Multi-access Edge Computing in 5G:

Multi-Access Edge Computing (MEC) is a crucial component of the 5G architecture. MEC is a cloud computing extension that takes applications from centralised data centres to the network edge, closer to end users and their devices. Bypassing the long-distance network path that traditionally separated the user and host, this effectively establishes a shortcut for content delivery between the user and host. This technology is not unique to 5G, but it is essential for its performance. Multi-access edge computing (MEC) provides cloud computing and IT services at the network edge. MEC reduces latency, improves user experience, and optimises network and service delivery. European Telecommunications Standards Institute (ETSI) has primarily developed the technical and architectural specifications for multi-access edge computing.

Virtualizing network functions is a necessary step toward 5G implementation, as it will streamline network operations, increase availability, and pave the way for the development of new services and capabilities. When it comes to 5G networks, MEC is one option to improve the consumer experience and maintain or increase speed and latency. MEC and 5G are able to collaborate to provide new applications and services. On a MEC platform, value-added services or "smart" applications offered over 5G are executed. For instance, an AI/ML application would be installed on the MEC platform. The radio access network (RAN) connects the user's device to the operator's core network. The RAN bridges the gap between the operator's network and the devices of its customers, allowing the operator's voice, data, and OTT services like video streaming or healthcare service.

1.6.1 Multi-access edge computing usage scenarios [6]:

- Data and video analytics
- Location tracking services for mobile devices
- Internet of Things (IoT) and IoT devices
- Augmented reality/virtual reality

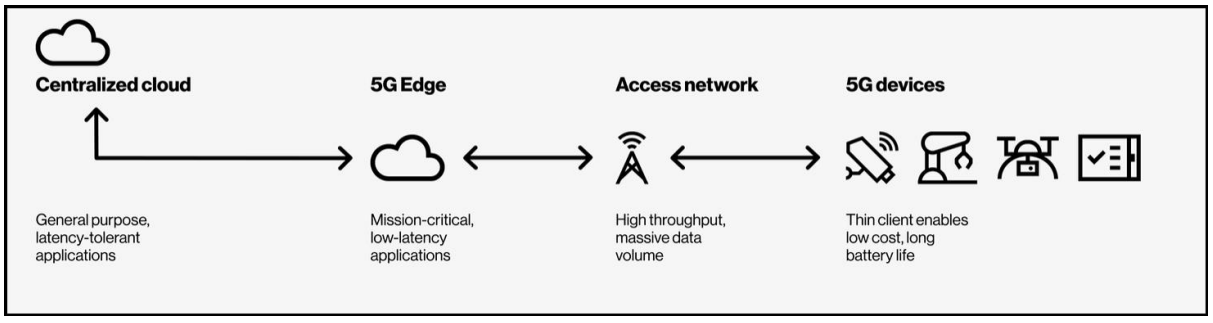

Figure 10 MEC Usage Scenarios [6]

1.7 Security in 5G:

By heavily utilizing cloud-based resources, virtualization, network slicing, and other upcoming technologies, 5G adoption delivers excellent performance improvements and a diversity of applications. A new set of vulnerabilities are exposed due to security attacks and makes it vulnerable. Security mechanisms relevant to 3GPP, namely the functional parts and interfaces, were the primary focus of the standardisation process. There were many security risks that were involved in 5g deployment. Enhanced security concerns for potential 5G rollout scenarios include:

Increased attack surfaces: 5G enables larger and more hazardous assaults since it can connect millions or perhaps billions of devices. The weaknesses in the current internet infrastructure are only going to get worse as time passes on. With 5G, the potential for more advanced botnets, privacy concerns, and rapid data extraction increases.

More IoT devices: Because security is rarely considered during the design phase, IoT devices have a high risk of being compromised. Every unsecured Internet of Things (IoT) gadget on a company's network is another entry point for hackers.

Decreased network visibility: With 5G, our networks can accommodate more people and more devices than ever before. More data will be flowing via the network. However, businesses may lack the network traffic visibility necessary to detect irregularities or assaults in the absence of a reliable wide area network (WAN) security solution such as Secure Access Service Edge (SASE).

Increased in 5G chain and software vulnerabilities: In the present and foreseeable future, 5G supply chains are constrained. Existence of vulnerabilities, especially when products are pushed to market, increases the likelihood of defective and unsecured components. 5G

mobile networks are much more reliant on software than previous mobile networks, which increases the danger of network infrastructure exploitation**.** Enhanced security concerns for potential 5G rollout scenarios include:

System-wide security (horizontal security)

- Network level
- Slicing
- Application-level security
- Confidentiality and integrity protection
- Interconnect (SBA)

5G function element deployments (vertical security)

- NFVi (virtualized or cloud native)
- Appliance based functions
- Distributed clouds and edge computing

2 Introduction to IoT:

The Internet of Things (IoT) includes a broad range of products and communication mechanisms. Today, IoT describes the idea of connecting everything to the internet. IoT's potential for new services and innovations makes it crucial. All items will be interconnected and capable of two-way communication. IoT includes all kinds of different technologies and every possible way to communicate between (virtual or physical) objects via the Internet. The breadth of this concept makes it rather complex because of the heterogeneity of components. Since every type of device may use specific hardware and software, a wide range of operating systems and applications must be considered. In some cases, the devices may not even have an operating system. For example, some devices only have a network interface, a driver, and an application generating (or sinking) data.

Typically, devices from various manufacturers speak different protocols. Occasionally, these protocols are confidential and hence unknown to the audience. Experience has shown us that secure protocols need open peer review to give a thorough evaluation and, as a result, gain widespread acceptance and implementation. Due to their usage of Internet Protocol (IP) at the network layer of the protocol stack, IoT devices increasingly share similar characteristics. These gadgets increasingly employ IP to facilitate Internet-based communication.

New technologies such as short-range wireless communications, RFID, and real-time localization are becoming increasingly widespread, allowing the Internet to infiltrate the physical world. The introduction of IPv6, the initiatives for porting the IP stack to embedded devices, and the defining WPAN enable the Internet of Things vision, which refers to a network of objects in which all items may be individually and universally addressed, recognized, and managed by computers. IoT is a combination of technologies that allows sensors and actuators to be connected to the Internet.

IoT can defined formally as “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network, often communicate data associated with users and their environments[5].”

The Internet of Things (IoT) is gaining popularity. In 2017, there were around 20 billion IoT-connected devices, the number has increased to 30 billion in 2020 and more than quadruple by 2025. Due to its limits, the expanding IoT presents cloud computing with several new challenges.

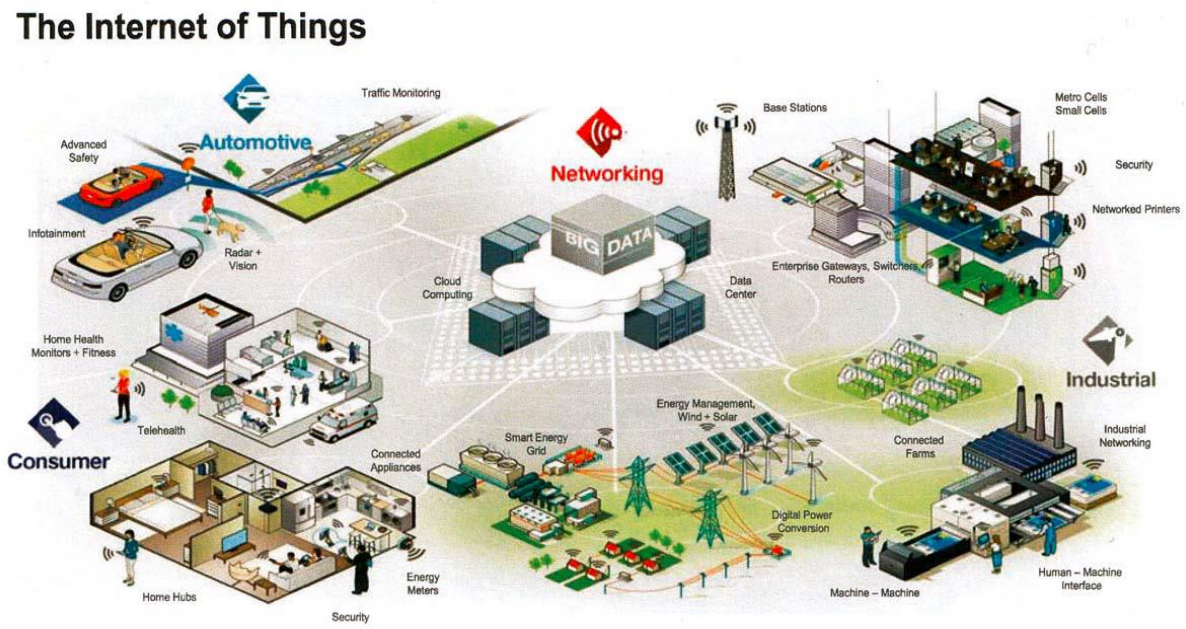

Figure 11 General Usages of IOT (Source: google images)

Kevin Ashton introduced the phrase Internet of Things in one of his presentations in 1999, as per AutoIDlabs. The Internet of Things signifies a global network of networked, uniquely addressable things based on common communication protocols. In the explanation of meaning, "things" refers to objects. The concept of "things" began with Radio-Frequency Identification (RFID) tags developed by Auto-ID Labs, a global network of university

research laboratories specialising in networked RFID and developing sensing technologies. Subsequently, more "things" concepts arose, including NFC tags, Wireless Sensor and Actuator Networks and Smart Items.

2.1 Characteristics of IoT:

- **Self-configuring:** The capability to configure themselves, to set up the networking, and to retrieve the most recent software upgrades with minimal human intervention.
- **Unique identity:** Every gadget has its own distinctive identifier, such an IP address, so that they may communicate with one another.
- **Interoperable communication protocols:** Maintain compatibility with a variety of communication protocols used by other devices and the underlying infrastructure.
- **Dynamic and self-adapting:** Devices should be in a dynamic environment where they can adapt to changes automatically with minimal or no human intervention.
- **Integrated into information network:** Devices should easily integrate with the other networks.
- **Interconnectivity:** Everything in the Internet of Things can be interconnected because of advancements in global connectivity and information infrastructure.

2.2 Generic block diagram of IoT:

An Internet of Things device could include a number of wired and wireless interfaces for establishing connections to different types of devices. Some of the interfaces are mentioned below:

- I/O interface for sensors
- Interfaces for Internet connectivity
- Memory and storage interfaces
- Audio and video interfaces

- Graphic interfaces
- Processor

Figure 12 Generic block diagram of an IOT device

2.3 IoT Communication Protocols:

IoT is heterogeneous in nature. The protocols for the Internet of Things (IoT) are a crucial component of the IoT technological stack. Hardware is meaningless without the protocols and standards for the Internet of Things. This is because it is IoT protocols that make it possible for all these devices to talk to one another and share data and instructions. Users are able to engage with and control devices based on the information and orders that are transmitted to them. In a typical IoT system, you'll find a wide variety of smart devices, protocols, and apps all working together. Devices and communication protocols may need to be modified for specific projects and use cases.

Experts have developed a framework for categorizing the various parts of an IoT architecture into separate groups, or "layers," to accommodate the wide variety of IoT systems and their respective uses. These layers facilitate interoperability and allow IT staff to focus on specific areas of a system that may require attention. This means that likelihood of interoperability across systems increases if each system adheres to the standard set of layers.

The Open Systems Interconnection (OSI) model, which describes seven distinct layers in a top-down architecture, is one of the finest foundations for understanding IoT layers. The term "top-down" refers to the method in which the layers are specified, beginning with the interface that an average user would have with an IoT system (such as a smartphone app or website) and ending with the underlying infrastructure (such as ethernet cables) that do the work of transmitting data. The seven layers of the OSI model are listed below,

- **Application Layer:** This layer incorporates the web and mobile apps used to communicate with IoT devices.
- **Presentation Layer:** In this layer, information gathered by IoT devices is encrypted and transformed before being delivered to the application layer.
- **Session Layer:** This layer acts like a timetable for information transfer between sources and destinations. For two devices to have a conversation within an IoT system, the system must first set up a time for that conversation, called a session.
- **Transport Layer:** The transport layer provides error control, segmentation flow management, and congestion control. It is similar to a company’s fleet of trucks, except that in this case the data moved is data packets rather than physical containers.

- **Network Layer:** This layer acts as the system's "post office," coordinating when and where information is transferred. Routers are an essential network layer component because they direct data packets to their final destinations**.**
- **Data link Layer:** This layer joins various devices to facilitate data flow at the network layer and corrects mistakes caused by anomalies or broken hardware at the physical layer.
- **Physical Layer:** Typically found at this level are infrastructure components such as ethernet cables, cell towers, base stations, and the like**.**

Since OSI is only a model in theory, it may not accurately portray some real-world IoT implementations. The seven OSI layers let IT teams narrow down the source of a mistake, much like a factory would be separated into distinct maintenance zones to facilitate locating and fixing problems with different units. Further, the OSI model provides a practical means of understanding the many aspects of an IoT network. Experts often summarize IoT architecture as a three, four, or five-layer model that may be further subdivided based on the Open Systems Interconnection (OSI) reference model.

Like the OSI model, a three-layer model includes an application layer. Next up is the internetwork or network layer. In the end, all of the sensors in an IoT system make up the perception/sensing layer.

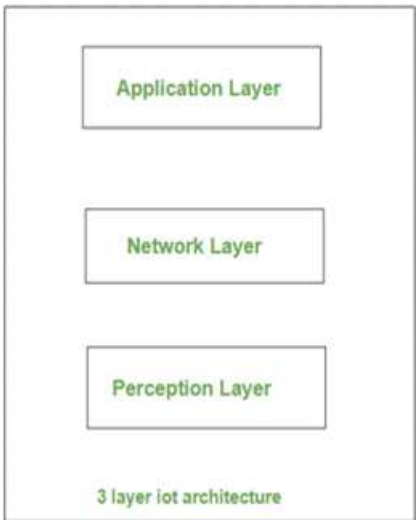

Figure 13 Generic 3 -layer Modelled IoT architecture

An OSI model is easy to compare to a four-layer model. The application layer of an OSI model comprises the application, presentation, and session layers. The transport layer and network/Internet layer facilitate the digital transmission of data. The physical network access layer includes ethernet cables, routers, modems, etc., and is the last. The four-layered model can be easily understood by comparing it with the OSI reference model, which is illustrated below.

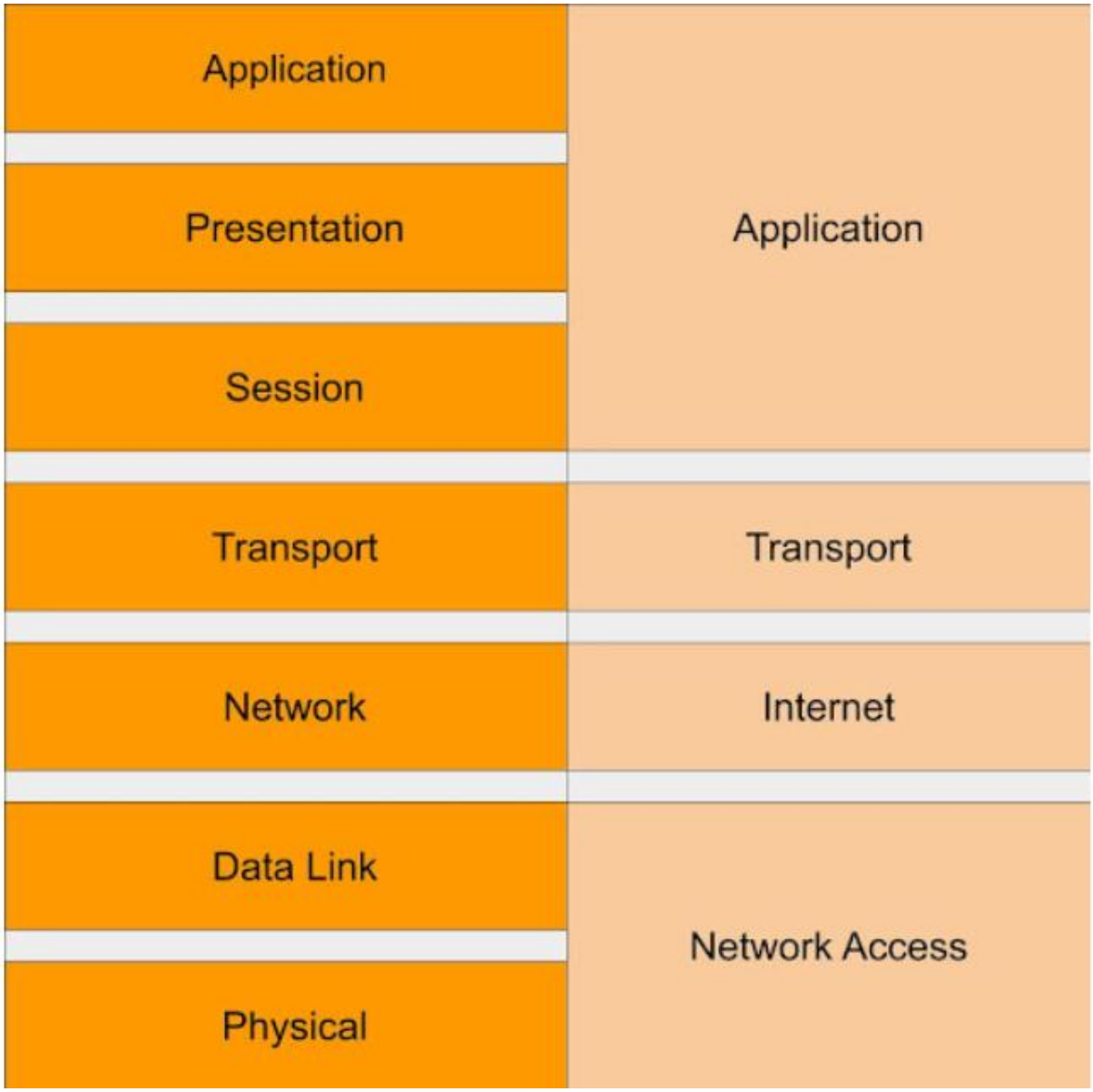

Figure 14 Generic Comparison of 4-layer model and OSI model. [7]

The final layer of a five-layer model is the business layer. You may also refer to this level as the "cloud database layer" or the "data analytics layer" when discussing the business layer. Here, sensor data is transformed into useful information. Most Internet of Things systems now includes a business layer due to the rise of data-driven upkeep and operations.

In most of the IoT devices four-layer model architecture is used and in this the IoT protocols are again categorized into two types:

- IoT data protocols (Presentation / Application layers)
- Network protocols for IoT (Datalink / Physical layers)

2.3.1 4 – layered IoT architecture and its components:

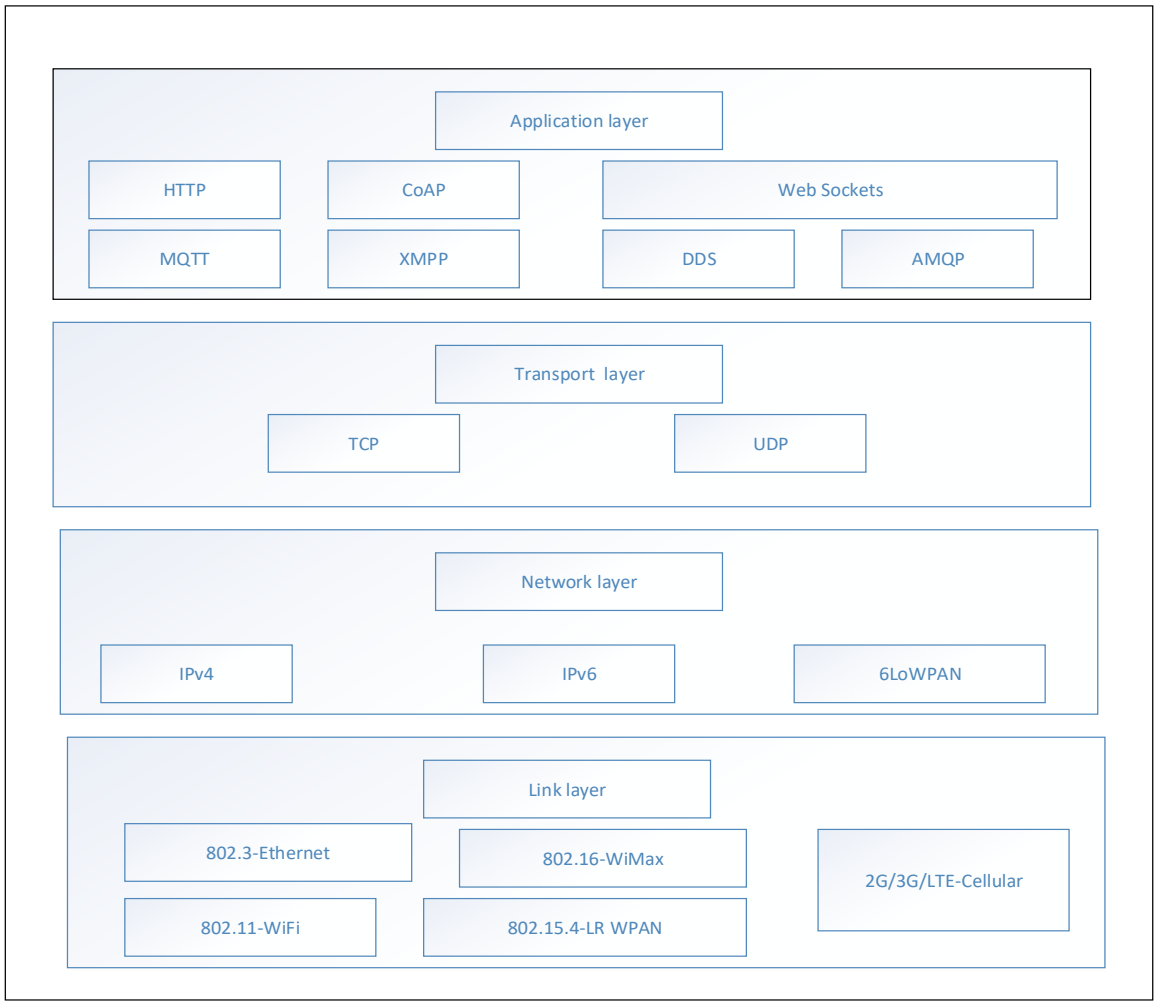

Figure 15 Generic flow chart of 4-layered model IOT architecture

2.3.1.1 Data Link Layer Protocols:

This layer is responsible for determining how data is physically sent via the physical layer of the network, also known as the medium, which can be copper wire, quacks genuine cable, or radio waves. Through the use of the following link layer protocols, the exchange of data packets takes place over the link layer**.**

- 802.3- Ethernet
- 802.11- Wi-Fi
- 802. 16- Wi-Max
- 802. 15. 4- LRWPaN
- 2G/ 3G/ 4G/5G- Mobile communication

2.3.1.2 Network or Internet Layer:

This layer is responsible of transmitting IP datagrams from the source network to the destination network. It addresses hosts and routes packets.

- **IPV4:** The most used Internet protocol with a 32-bit addressing system that offers more than 4 million addresses; nevertheless, as the number of digital devices that can connect to the internet increased, IPv4 ran out of available addresses in 2011.
- **IPV6:** IPV6 is the successor of IPV4, which features an addressing scheme that consists of 128 bits and enables 3.4 x 1038 addresses to be used. This is an enormous amount, which is adequate for IoT purposes.
- **6LowPAN:** This protocol translates to Internet Protocol Version 6 across a low-power wireless personal area network. It also makes IP Version 6 accessible to low-power devices that have a restricted capacity for processing data. It offers data transfer speeds of up to 250 KBPS at the transport layer.

2.3.1.3 Transport Layer Protocol:

The transport layer protocol enables bidirectional message flow across established connections (using TCP handshakes or UDP without handshakes). Error handling, traffic segmentation, and congestion management are all services provided by the transport layer.

1. **Transmission Control Protocol:**
    - Web browsers, email clients, and file transfer services employ this protocol at the transport layer. This protocol is stateful and focuses on establishing and maintaining connections. The Transmission Control Protocol (TCP) ensures the secure sending of packets and includes error detection to prevent the transmission of duplicates and the retransmission of missing packets. It can regulate the flow of information so that the load on a receiver's system isn't too great, and it can assist in preventing networks from being overloaded. Since it is a connection-based protocol, the initial configuration is necessary.
    - It can regulate the flow of information so that the load on a receiver's system isn't too great, and it can assist in preventing networks from being overloaded. Since it is a connection-based protocol, the initial configuration is necessary.
2. **Unit Datagram Protocol:**
    - As this is a connectionless protocol, there is no preliminary configuration needed. In time-critical situations, it proves to be quite helpful.
    - When exchanging only a few bytes of data at a time and without needing the full functionality of a fully established connection, this method is ideal. This is a stateless, transaction-focused protocol. However, it lacks features such as assured delivery order, removal of duplicates, and so on.

2.3.1.4 Application Layer:

Protocols at the application layer specify how one network talks to another. The application layer protocol encodes the application data, usually stored in files, and then the transport layer protocol encapsulates the application data for transmission across the network. Port numbers are used to address applications, such as port 80 for HTTP and port 22 for SSH.

1. **HTTP (Hyper Text Transfer Protocol):**
   - It's the foundation of the WWW, or the World Wide Web. Users may use functions like GET, PUT, POST, DELETE, HEAD, OPTIONS, etc. The protocol operates in a request-response mode.
   - As each HTTP request is autonomous from the others, the protocol may be described as stateless. HTTP is built on TCP and may be used by any client-side program, such as a web browser or mobile app. Because of its high price tag, short battery life, excessive power consumption, and heavyweight, the HTTP protocol is not favoured as an IoT standard.
2. **CONSTRAINT APPLICATION PROTOCOL (COAP):**
   - This protocol is used for machine-to-machine communication. It is designed to function in environments where resources, including devices and networks, are limited. It operates on top of UDP and has a request-response mechanism. It was built to talk to the HTTP protocol. Delete, Put, and Post commands are supported.
   - While every IoT gadget may use the internet's framework, it's generally excessively hefty and power-hungry. Many in the IoT community consider HTTP unsuitable for IoT. CoAP overcomes this restriction by adapting the HTTP paradigm for limited devices and networks.

- It supports multicast, has low overheads, and is straightforward to use. CoAP is suited for resource-constrained devices like IoT microcontrollers and WSN nodes. It's often employed in smart energy and building automation.

3. WEB SOCKETS:

- To facilitate two-way data exchange between a client and server, WebSockets use a single TCP/IP socket connection for both transmitting and receiving data. It is built on the TCP protocol. It maintains the TCP connection between the client and server while a continuous stream of messages is sent between them. In this context, "client" might refer to a web browser, a smartphone app, or an Internet of Things device.
- WebSocket, like CoAp, uses a standardized connectivity protocol to streamline the administration of connections and bidirectional communication across the internet. WebSocket can be used in an IoT network to provide continuous data communication between devices. Therefore, its most popular use is in client- and server-oriented environments.

4. MESSAGE QUEUE TELEMETRIC TRANSPORT (MQTT):

- The MQTT protocol is based on a publish/subscribe architecture. MQTT is a lightweight IoT data protocol.
- A client, in this case, is an IoT device that connects to a server, also known as an MQTT broker, and publishes messages to topics on the server. The communications are delivered to the consumers who have subscribed to the subjects by the broker. MQTT functions effectively in low-resource settings, such as those with limited processing power, low bandwidth, and low memory.

- IoT data protocols address unstable communication networks. Over the past several years, more tiny, inexpensive, and low-power gadgets have entered the IoT network, demanding this.
- MQTT, a popular IoT standard with industrial applications, doesn't offer a specified data representation and device management structure mode. Data and device management is platform- or vendor-specific. The protocol lacks security; hence device and application security must be handled.

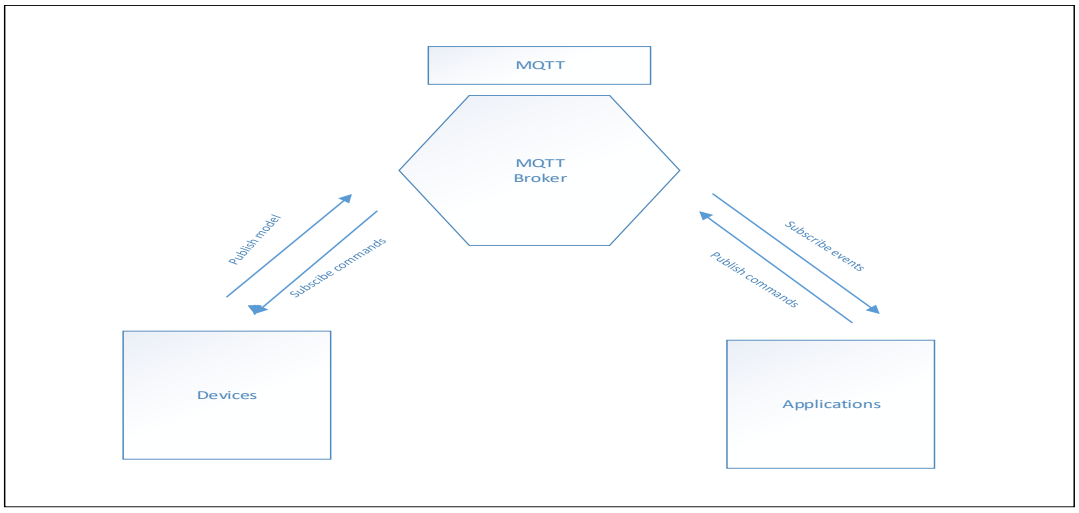

Figure 16 Generic MQTT Protocol

5. EXTENSIBLE MESSAGING PRESENCE PROTOCOL (XMPP):

- Network entities utilize this protocol to carry out communication in realtime as well as the streaming of XML data.
- XMPP is the engine that powers various services, such as messaging, gaming, multi-party chat, audio or video conferencing, and more.
- It makes it possible to send chunks of XML data from one network to another network in a timeframe that is very close to being considered real-time.

- XMPP is an example of a client-server architecture that uses decentralized protocols.

6. DATA DISTRIBUTION SERVICE:

- It is a protocol for exchanging information between computers and other devices. DDS, like other scalable IoT protocols, facilitates IoT communications of high quality.
- DDS follows a publisher-subscriber mechanism, just like MQTT. The data distribution role is played by the publisher, while the data reception role is played by the subscriber.
- It has a wide range of potential deployment scenarios, from the cloud to small devices. In other words, it's ideal for use in embedded and real-time systems. DDS in contrast to MQTT, supports cross-platform, system data sharing. DDS is widely recognised as the pioneering open international middleware IoT standard.

7. ADVANCED MESSAGE QUEUING PROTOCOL:

- It is a free and open protocol for sending and receiving messages in the business world. It is compatible with both one-to-one and group communication. Publishers send messages to an exchange, which subsequently sends copies to waiting areas known as queues. The broker can hand over messages to the consumer, or the consumer can get them from a queue.
- AMQP is widely used in industries that rely on server-based analytical systems, such as banking, because of its excellent security and dependability in these conditions. Its application is limited in other contexts.

- AMQP is too resource-intensive to be used by low-powered IoT sensors. Therefore, its implementation in the Internet of Things (IoT) remains restricted.

2.4 IoT Communication Models:

Internet of Things (IoT) devices are widespread and will eventually provide circulatory intelligence. Knowing how different Internet of Things devices talk to one another is vital and helpful from an operational perspective. The IoT communication concepts are valuable. The IoTs make it possible for devices to communicate with one another and with other devices, users, networks, and services at any time, from any location. There are four types of communication models that are used for various purposes in IOT, and they are listed below.

- **Request-Response model:** This model follows client and server architecture. In the Request-Response model, the client initiates contact with the server by making a request, and the server then responds to the first request. When the server gets the request, it decides how to answer, goes out, gets the data and any other resources it needs, and then prepares and transmits the response to the client.
- **Publish-Subscribe model:** The Publish/Subscribe model comprises media outlets, brokers, and subscribers. Publishers distribute content to subscribers governed by brokers. Customers are invisible to publishers. Clients sign up for the services offered by the broker who handles the topics. When the broker gets messages on a specific topic, it processes them. After the broker gets the data from the publisher, it is distributed to various users.

- **Push-Pull model:** Data publishers, consumers, and queues form the push-pull model. Publishers and consumers are unaware of each other. Publishers push messages/data onto the queue. On the other side, consumers pull data from the queue. Thus, the queue buffers messages when publisher and consumer data push and pull rates diverge. Queues separate producer-consumer messaging. Queues also buffer data when producers push faster than consumers draw.
- **Exclusive pair model:** An exclusive Pair is a bidirectional approach that allows full-duplex communication between the client and the Server. The connection is always active and will stay open until the client issues a command asking for the connection to be closed. The Server maintains a record of all the connections established since it was started. This form of connection has a full state, and the Server is aware of all connections that are currently active. The application programming interface (API) for WebSocket-based communication is built entirely on this concept.

2.5 IoT Challenges:

The Internet of Things has introduced various obstacles, which are fueling an increased interest in edge computing as a potential solution to problems of this nature. The following is a list of some of these difficulties:

- **Low Latency:** Both industrial control systems and Internet of Things applications frequently need a low latency and jitter (within a few milliseconds) level of performance. This criterion does not apply to the Edge computing concept in any way.
- **Limited Resources:** Some Internet of Things gadgets (sensors, drones, cars, etc.) needs to be more constrained in their capabilities. This means they cannot connect directly to the Cloud, as such links often need elaborate protocols or intensive

computing. Therefore, devices with limited resources must rely on an intermediary interface layer to establish a connection to the Cloud.

- **Intermittent Connectivity:** Network connectivity might be spotty for some IoT gadgets (e.g., vehicles and drones). This makes it challenging to offer such devices with constant access to cloud services. Therefore, it is necessary to rely on a tier of devices in between the two extremes in order to mitigate or eliminate the issue.
- **Context Awareness:** Many Internet of Things applications, such as vehicular ad hoc networks and augmented reality, require access to and processing of local context information (for example, the user's position or the network's conditions). This particular offering does not entail a centralized approach to edge computing due to the physical distance between IoT devices and central computing.
- **Geographical Distribution:** The vast majority of Internet of Things devices that need access to computing and data storage resources are dispersed across huge geographical regions. It is thus challenging to choose a location for the cloud infrastructure that satisfies the requirements of all Internet of Things application criteria. It would be helpful to have a layer of devices between these two extremes.
- **High Network Bandwidth:** The ever-increasing number of linked Internet of Things devices generates an ever-increasing volume of data. A network of an extraordinarily massive scale is required to upload all of this data to the cloud. Bandwidth is frequently wasted or forbidden from use (e.g., due to concerns about data privacy). As a result, the data created at the edge of the network must frequently be stored and processed locally to avoid involving the cloud.

- **Industrial Technology and Operational Technology:** With the emergence of Industry 4.0, Operational Technology (OT) and Information Technology (IT) have been integrated into industrial networks. Because of this shift, the business now has different objectives and must adjust its structure accordingly. In today's cyber-physical systems, uptime and security are always top concerns since downtime may result in significant financial losses for businesses and pointless headaches for their customers. This makes it difficult to update the system's hardware and software. As a result, it's essential to adopt a brand-new design that, in the long run, does away with the requirement of constant system updates.

2.6 CyberSecurity in IoT:

Emerging concerns regarding the privacy and security of IoT are one of a kind. Firewalls, intrusion prevention systems (IPSs), and intrusion detection systems (IDSs) that provide perimeter-based protection are the primary components of modern cybersecurity solutions. These solutions are designed to safeguard both organizations and individual customers. Unfortunately, this paradigm is no longer enough to handle the new security issues posed by the Internet of Things (IoT).

Security is crucial for virtually all IoT applications that have been deployed or are in the process of being deployed. IoT applications are fast expanding and reaching the majority of current industries. Despite the fact that operators offer many IoT applications using current networking technologies, a number of these apps require more strict security support from the technologies they employ[6].

Each application in the Internet of Things has four distinct layers: the sensing layer, the network layer, the middleware/transport layer, and the application layer. Each of these levels employs a different set of technologies in an IoT application, each with its own set

of problems and risks. The graphic below illustrates the four levels, each having different technology, devices, and applications.

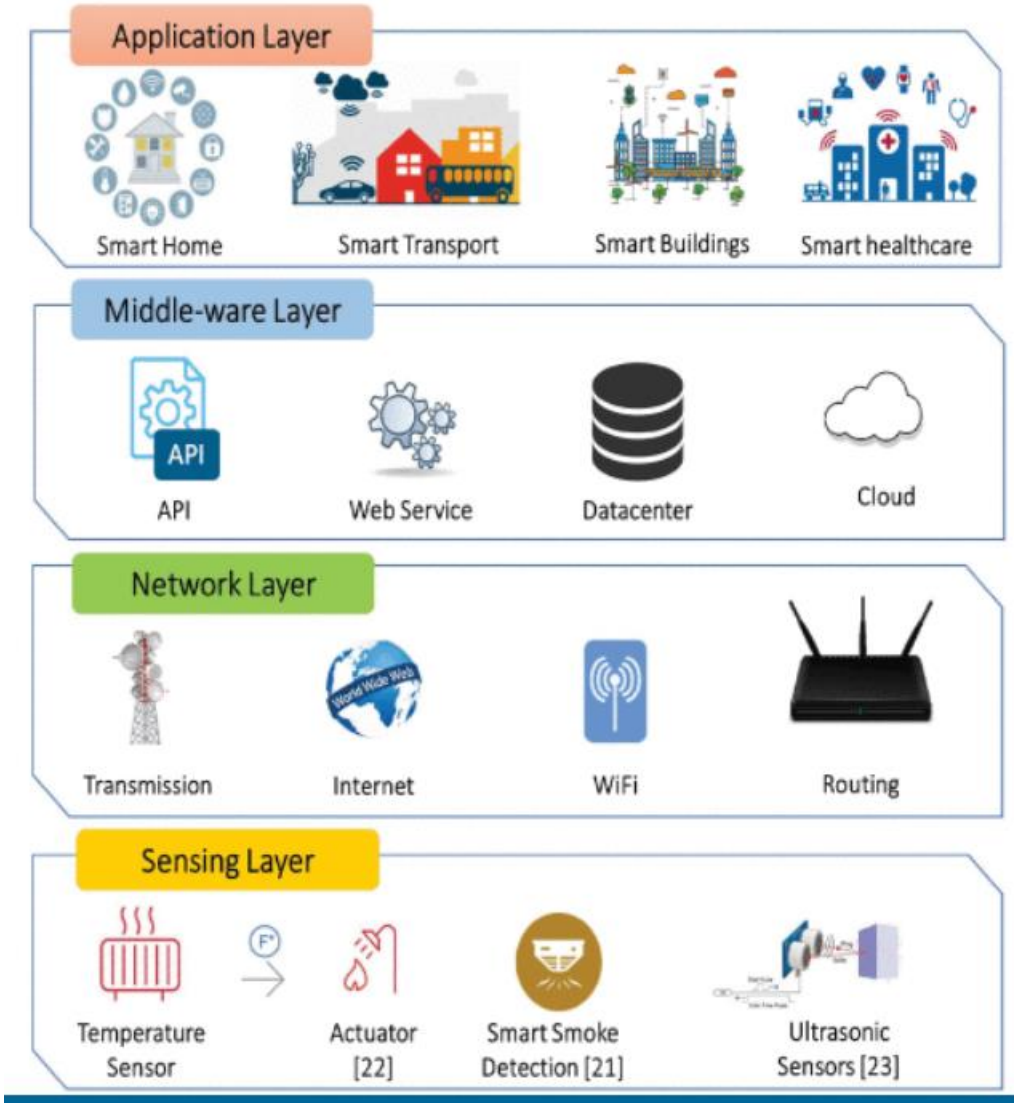

Figure 17 Different applications at each layer in IOT [8]

The figure that follows illustrates the potential assaults on these four layers. The picture also illustrates the particular concerns about data protection that are connected to the gateways that link the different layers.

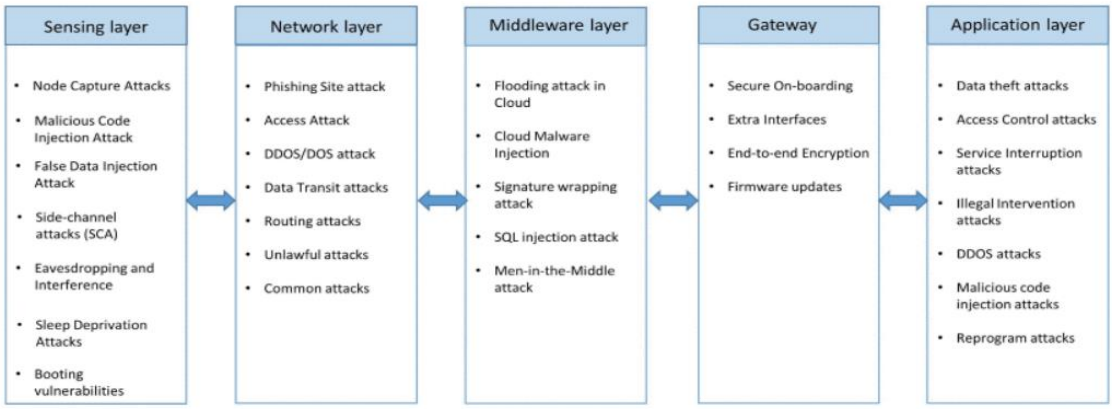

Figure 18 Different types of attacks that take place in each layer [7]

2.6.1 Security attacks at Sensing Layer:

IoT sensors and actuators are the primary focus of the sensing layer. Sensors gather information about the physical world around them. Whereas actuators take action in response to that information. Ultrasonic sensors, cameras, smoke detectors, temperature and humidity monitors, and so on are only a few examples of the many types of sensors available. Physical environment sensors can be mechanical, electrical, electronic, or chemical. RFID, GPS, WSNs, RSNs, etc., all function as examples of sensing layer technologies utilised in various IoT applications. Some of the security attacks that are possible at this layer are :

- Node Capturing
- Malicious Code Injection Attack
- False Data Injection Attack
- Side-Channel Attacks (SCA)
- Eavesdropping and Interference
- Sleep Deprivation attacks
- Booting Attacks

2.6.2 Security attacks at Network Layer:

The information obtained from the sensing layer is then sent to the computing unit so that it may be processed. This is the primary responsibility of the network layer. The following list details the primary concerns about data protection at the network layer.

- Access Attack
- DDoS/Dos attack
- Data transit Attacks
- Routing Attacks
- Phishing Side attack

2.6.3 Security attacks at Middleware Layer:

Middleware is employed to facilitate communication between the IoT's network layer and its application layer. Middleware has the potential to offer substantial computational and storage resources. To meet the needs of the application layer, APIs are provided by this layer. The middleware layer is generated by brokers, permanent data storage, queuing systems, machine learning, and similar technologies. The middleware layer is necessary for a secure and stable IoT application, but it may also be attacked in several ways. Because these attacks target the application's middleware, the entire IoT application is at risk of being compromised. Middleware security issues also include protecting databases and the cloud. Some of the potential attacks that may be made against the middleware layer are listed below.

- Man-in-the-Middle Attack
- Signature Wrapping Attack
- Cloud Malware Injection
- SQL Injection Attack
- Flooding Attack in Cloud

2.6.4 Security issues at Gateway:

The gateway is a comprehensive layer that facilitates the interconnection of many endpoints, including users, devices, and cloud resources. Gateways also aid the provision of hardware and software solutions for IoT devices. Decrypting and encrypting IoT data, as well as interpreting protocols for inter-layer communication, are all functions performed by gateways. Today's IoT systems are highly complex, involving a variety of gateways and protocols, such as LoraWan, ZigBee, Z-Wave, and TCP/IP. Several IoT gateway security problems are listed below.

- End-to-End Encryption
- Extra Interfaces
- Secure onboarding
- Irregular Firmware updates

2.6.5 Security issues at the Application Layer:

The application layer is responsible for communicating with and serving the end users. This layer contains the Internet of Things applications, such as smart homes, water meters, smart cities, smart grids, etc. Particular security concerns, such as data theft and privacy invasion, are unique to this layer. Similarly, the security concerns at this level vary depending on the application. There is often a sub-layer between the network layer and the application layer in many IoT systems; this layer is also referred to as the middleware layer or the application support layer. The support layer supports the business services and intelligent resource allocation and computation. Below are some of the most common application layer security concerns.

- Data Thefts
- Access Control Attacks

- Service Interruption Attacks
- Malicious Code Injection Attacks
- Sniffing attacks
- Reprogram attacks.

3 Introduction to Cloud Computing:

The National Institute of Standards and Technology (NIST) provided a definition of Cloud Computing that outlined its major characteristics. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [7]

While the idea of cloud computing isn't new, it has gotten a lot of attention in recent years with platforms like AWS, Azure, and GCP gaining significant traction among cloud users. Cloud computing allows consumers to access and utilize these services whenever they need them without needing costly equipment or dedicated IT professionals. Because of this, it is a cost-effective and versatile solution that enterprises of any size can use. The use of cloud computing may be advantageous in many different ways. It can give scalability, flexibility, and cost savings, among other benefits. It enables businesses to concentrate on their primary activities while cloud providers take care of the infrastructure and upkeep of their information technology systems. National Institute of Standards and Technology (NIST) introduced cloud computing with five essential characteristics:[8] .

- on-demand self-service
- rapid elasticity or expansion
- broad network access
- resource pooling
- measured services

Cloud computing features can be depicted by the below illustration.

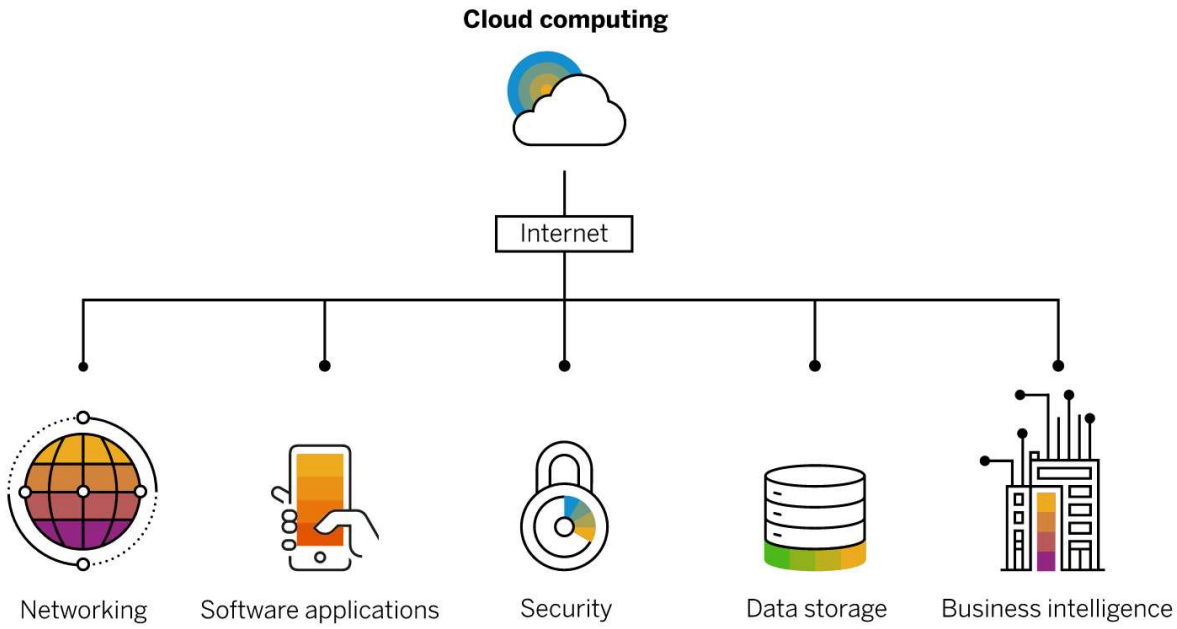

Figure 19 Features of Cloud Computing (Source :Google images)

3.1 Cloud Computing Service Models:

Cloud computing can be divided into three main categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

1. **IaaS (Infrastructure as a Service):**

   This type of cloud computing uses the internet to deliver virtualized computer resources to users. AWS, Microsoft Azure, and Google Cloud Platform are a few examples of IaaS. IaaS providers often make available a wide variety of computing resources that may be supplied and scaled according to the customer's requirements at any given time.

   Users can rapidly develop and administer their virtual infrastructure with this help, eliminating the requirement for them to acquire and maintain expensive hardware. The user does not manage or have control over the underlying cloud infrastructure. Still, they have control over the operating systems, storage, and applications installed,

as well as some restricted control over specific networking components (e.g., host firewalls).

Typically, when it comes to virtual infrastructure configuration and management, IaaS providers will give a broad range of possibilities, such as: Virtual machines, security, storage, networking, load balancing, Automation, backup and disaster recovery, monitoring and analytics. Instead of making a substantial initial investment in hardware, many IaaS providers provide a pay-as-you-go pricing model, where customers only pay for the resources they utilize. Because of this, infrastructure as a service (IaaS) is a viable choice for businesses of all sizes, especially those who need to deploy and scale their IT infrastructure rapidly.

2. **Platform as a Service (PaaS):**

PaaS is an all-inclusive application development platform hosted in the cloud that offers programmers a place to create, test, and release their software. You may choose the cloud services and capabilities you wish to utilize as a developer and pay for them on a subscription or as-you-go basis with PaaS. One such platform is Google App Engine1, which provides Python and Java runtime environments and APIs for apps to interact with those environments. In addition to being a cloud computing service, Microsoft Azure can be viewed as a platform service since it offers developers access to the Azure cloud and an application programming interface (API).Heroku and AWS Elastic Beanstalk are also examples of PaaS.

Making an app for the cloud is similar to making one for traditional web servers in that both need programmers to build and deliver scripts to a distant server. The final product is a user-facing web app. PaaS differs from IaaS because it can incorporate supplementary services to ease creating, deploying, and running of applications, such

as scalability, monitoring, and load balancing. In addition to login and e-mail services, PaaS often provides access to user interface components.

PaaS services are also defined by their ability to supply APIs for data metering and invoicing. Using usage-based invoicing and metering makes it simpler for app creators to launch a revenue model based on user activity. Such aid allows developers and providers to profit financially while facilitating integration and maintenance of ties between end users, developers, PaaS, and any lower-level suppliers. PaaS providers typically offer a wide range of tools and services that can be used to create and deploy web and mobile applications such as development environment, Application hosting, Databases, application management, security and integration.

3. **Software as a Service (SaaS):**

Software as a Service, often known as SaaS, is a paradigm for delivering software in which an application for the program is hosted by a third-party provider and then made accessible to clients through the internet. Customers using the software as a service (SaaS) models do not have to worry about downloading, installing, and updating the program on their computers because it is all handled by the service provider. Instead, users pay a recurring charge (usually monthly or annually) to access the product.

With SaaS, businesses can access and utilize software in a flexible and scalable manner. They do not have to make expensive infrastructure, investments or handle software upgrades and maintenance. As companies search for methods to enhance their productivity while simultaneously lowering their expenses, SaaS adoption rate is rising. Email, customer relationship management (CRM's) such as Salesforce, ServiceNow, and human resource management (HRM's) are all examples of software

that may be provided as a service. For its flexibility, cheap cost, and simplicity of use, software as a service (SaaS) is becoming increasingly popular among enterprises. Given the limitations of the provider's data center, the creation and testing of applications under this paradigm are theoretically more straightforward. Furthermore, this strategy ensures a steady stream of revenue for the software vendor, which might be more cost-effective in the long term, including for the company's profit margin. Both consumers and suppliers of cloud services can benefit from this SaaS model.

In the below illustration it is easy to tell each type of services that are managed by application developer and cloud provider in all three cloud service models .

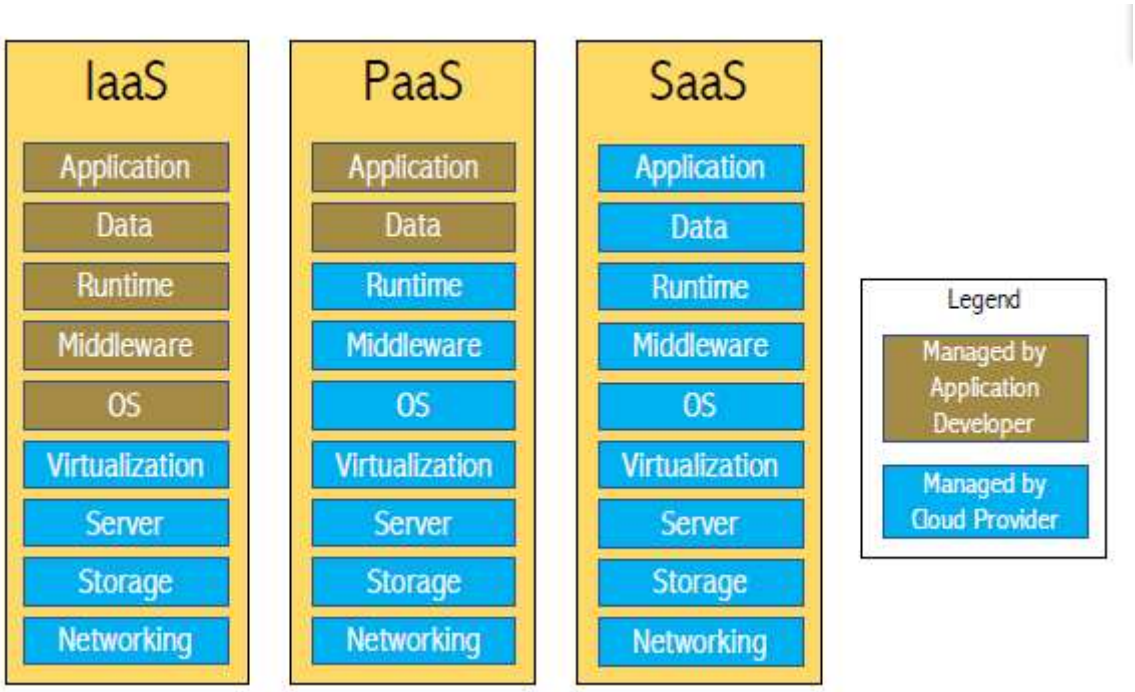

Figure 20 Classification of Cloud Service Models [9]

3.2 Cloud Computing Characteristics:

The following is a summary of some of the most important qualities that cloud computing possesses.

- **On-demand self-service:** The usage of cloud computing enables users to dynamically deploy computer resources, such as virtual machines and storage space, according to their specific requirements. Users can accomplish this using an API or a web-based interface, and they do not need the consent or support of a centralized IT department. Because of this, the provisioning of resources may be done with more flexibility and agility.
- **Broad network access:** Users can access their data and apps from any location as long as they have an internet connection due to the accessibility offered by cloud computing resources, which can be accessed across a network such as the internet. This enhances mobility and remote work.
- **Resource pooling:** In cloud computing, resources are shared across several users by being compiled into a single pool and then distributed according to their individual needs. Because of this, there is the potential for increased productivity and cost reductions, as there will be less wastage of resources**.**
- **Rapid elasticity:** The usage of cloud computing makes it possible to quickly scale the number of available resources up or down, depending on the users' requirements. This enables a greater degree of flexibility and the capacity to adapt to shifting needs swiftly.
- **Measured service:** It is feasible to keep tabs on and divulge information on the use of resources following the kind of service that is rendered. This is especially significant

for services that need a fee per use, also known as pay per user, since it provides excellent clarity between the service provider and the client.

- **Scalability:** The cloud allows the infrastructure to grow or shrink based on the users' needs. This enables a greater degree of flexibility and the capability of simply managing growing traffic and workloads.
- **Flexibility:** Storage, computation, and application hosting are just a few of the many services that may be provided by cloud computing. As a result, people have more options to choose the best answer to their task.
- **Cost-effective:** By removing the need to buy and maintain costly hardware, cloud computing helps to lower the overall cost of IT infrastructure and operations. On the other hand, clients only pay for the resources they use, which reduces overhead and allows for more customization.

3.3 Cloud Computing Architecture:

Cloud computing architecture describes the structure and operation of a cloud computing system, including all of its parts and the connections between them. When it comes to cloud computing, NIST breaks out the entities, their processes, and the services they offer. The figure is intended to assist in the grasp of cloud computing standards, requirements, features, and applications by representing a high-level generic architecture.

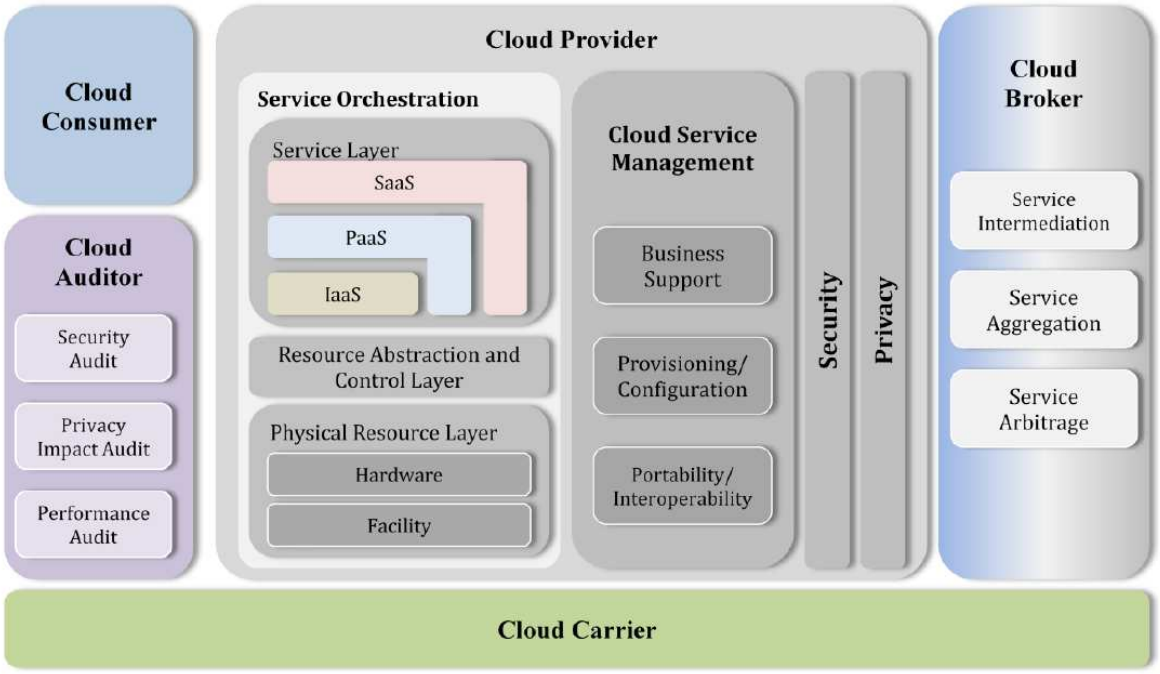

Figure 21 NIST Reference Cloud Computing Architecture[9]

The NIST cloud computing reference architecture (illustrated in Figure) identifies five key participants: the cloud consumer, the cloud provider, the cloud carrier, the cloud auditor, and the cloud broker. In cloud computing, each "block" represents a user or service provider who contributes to or completes a specific transaction, process, or set of tasks. The Five key entities are defined below.

- **Cloud Consumer:** A person or organisation that utilises the services offered by Cloud Providers and has a commercial relationship with such providers.
- **Cloud Provider:** A person, organization, or entity that is accountable for making a service accessible to people that are interested in receiving it.
- **Cloud Auditor:** A third-party organization that is capable of conducting independent evaluations of cloud services, information system operations, performance, and the level of security provided by the cloud deployment.

- **Cloud Broker:** An organization is responsible for managing the use, performance, and delivery of cloud services and facilitating the relationship-building process between cloud providers and cloud users.
- **Cloud Carrier**: A third party that acts as an intermediary to facilitate connectivity and the transmission of cloud services between cloud providers and cloud users.

The five key entities of NIST cloud computing architecture are discussed in detail below.

3.3.1 Cloud Consumer:

The cloud consumer is the cloud service's most essential asset. When an organization or a person enters a service agreement with a cloud provider, they are considered customers. A customer of the cloud can peruse the cloud provider's service catalogue, make a service request, establish a service contract, and begin using the service. There has to be a precise payment plan that considers the cloud user's demand for the service. SLAs are necessary for cloud users because they establish the technical performance standards that a cloud provider must meet. Service-level agreements (SLAs) can specify service quality, security, and consequences for performance failure.

A cloud service provider may need its clients to adhere to certain constraints and duties that are not explicitly stated in the SLAs. Customers can switch to a different service provider that offers better rates and terms when using the cloud. A cloud provider's price policy and service level agreements (SLAs) are usually not adjustable. However, this is only sometimes the case, especially if the client intends to use the service heavily and can thus negotiate more favourable terms. Below are some examples of how the activities and use cases of cloud customers might vary based on the services they subscribe to.

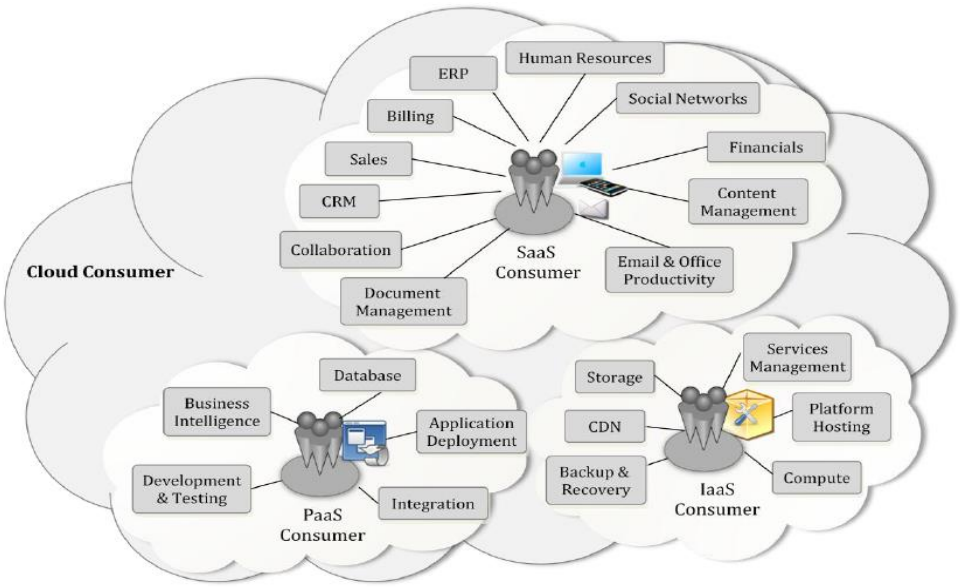

Figure 22 Services Available to a Cloud Consumer[9]

- **Consumers of SaaS:** Software-as-a-service applications are hosted in the cloud and made available to users across a network. Customers of software as a service (SaaS) can be any group with access to the program for its members, any individual with access to the software, or any group with access to the software responsible for configuring the software for end users. Customers of software as a service model may be charged based on the number of end users, the length of time data is held, the amount of data saved, the network bandwidth consumed, or any combination of these factors.
- **Consumers of PaaS:** PaaS cloud customers can utilize the cloud provider's tools and execution services to create, test, deploy, and manage cloud-hosted applications. PaaS users can be application developers writing and deploying app code, app testers deploying and testing apps in the cloud, app publishers distributing apps through the cloud, and app managers setting up and monitoring app performance across a network. The amount of computing, database and network resources that a PaaS application requires will vary.

- **Consumers of IaaS:** Virtual machines share storage space on the network, and other networking and computing resources are all made available to customers of an IaaS, allowing them to deploy and execute whatever software they choose. Infrastructure as a Service (IaaS) users might include programmers, administrators, and Executives who use the service to build, deploy, and keep tabs on their company's IT infrastructure. Consumers of IaaS are given access to these computing resources and are billed following the amount or duration of the resources consumed. This includes CPU hours virtual machines use, data storage volume and duration, network bandwidth used, and the number of IP addresses used during specific time intervals.

3.3.2 Cloud Provider:

A cloud provider can be an individual or a company, and they are the ones that provide the service to customers. Cloud Services are provided by a Cloud Provider, who is responsible for acquiring and maintaining the requisite computer infrastructure, running the cloud applications associated with the services, and coordinating the delivery of these services via network access on behalf of Cloud Users. Five main categories best illustrate a cloud service provider's work. Service deployment, service orchestration, cloud service administration, security, and privacy are all areas where a cloud provider is active.

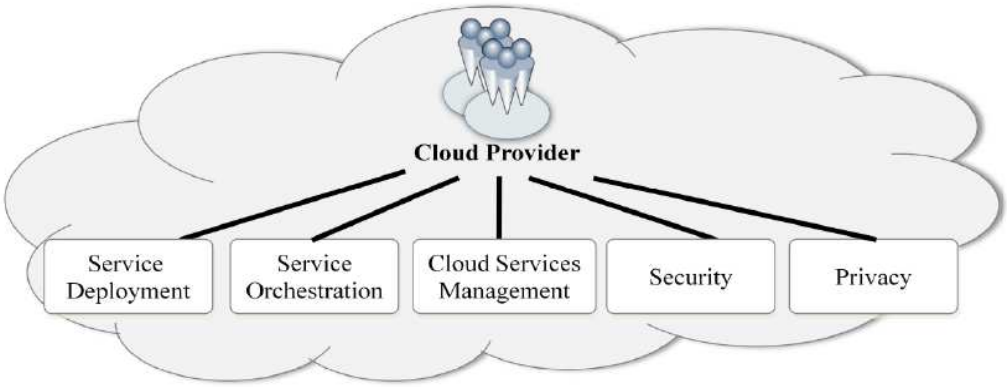

Figure 23 Services Available to a Cloud Provider[10]

- **Providers for SaaS:** Software as a Service relies on cloud infrastructure, which the cloud provider sets up, configures, manages, and updates so that it can deliver services to cloud clients at predetermined SLAs. The SaaS provider manages and administers the underlying infrastructure and apps, whereas cloud customers have limited access to the applications backend.
- **Providers for PaaS:** The Service Provider (CSP) is responsible for maintaining and operating the requisite hardware and software to deliver PaaS, which includes the platform's runtime environment, databases, and other middleware. Tools like integrated development environments (IDEs), cloud product development versions, software development kits (SDKs), deployment and management tools, etc., are typically provided by the PaaS Cloud Provider to aid the growth, deployment, and management processes of the PaaS Cloud Consumer. The PaaS Cloud User has control over the platform's apps and maybe some of the hosting environment's settings but has little to no control over the platform's underlying network, servers, OS, or storage**.**
- **Providers for IaaS:** The Cloud Service Provider purchases the hardware (servers, networks, storage, and infrastructure) that supports the IaaS service. The Cloud Provider operates the software necessary to provide computing services available to the IaaS Cloud

User via service interfaces and computer resource abstractions, such as virtual machines and virtual network interfaces. In return, the IaaS Cloud Consumer uses these resources for their computing tasks, such as running a virtual machine. The more software components in an application stack, including the operating system and network, the greater the capability of the IaaS Cloud Consumer, in contrast to the SaaS Cloud User or the PaaS Cloud User. In contrast, the IaaS Cloud Provider owns and operates the servers, networks, storage devices, host operating systems, and virtualization hypervisors that enable the supply of these infrastructure resources.

3.3.3 Cloud Auditor:

A party that can undertake an unbiased study of controls on cloud services to provide an opinion regarding those services is known as a cloud auditor. Audits are carried out to determine whether or not standards have been met through the evaluation of objective evidence. A cloud auditor can examine the services a cloud provider provides with regard to various criteria, including security controls, privacy impacts, performance, and so on. Federal agencies can benefit from privacy impact audits in many ways, including helping them comply with privacy laws and regulations and ensuring confidentiality, integrity, and availability of personal information.

3.3.4 Cloud Broker:

The convergence of cloud services might become too much for specific customers to manage as cloud infrastructure develops. A cloud user can make a service request for cloud services through a cloud broker rather than by contacting a cloud provider directly. A cloud broker is a third-party intermediary that mediates negotiations between cloud service providers and end-users to ensure cloud services security, privacy, and performance. Commonly, a cloud broker will offer three types of services:

- **Service Intermediation:** A cloud broker can improve service by expanding its core functionality and offering new features to its audience. Management of cloud service access, identity management, performance monitoring, strengthened security, etc., are all areas that might benefit from the upgrade.
- **Service Aggregation:** When using a cloud broker, several services are combined into a single one. The broker ensures secure data transfer between the cloud client and many cloud service providers and provides data integration services.
- **Service Arbitrage:** The process of service arbitrage is quite similar to service aggregation, except that the services aggregated are flexible. A broker who engages in arbitrage of services does so by selecting services from many providers. A cloud broker, for instance, may utilize a credit rating service to determine which agency has the highest score and then hire that one.

3.3.5 Cloud Carrier: A cloud carrier is a third party that facilitates communication and transport between cloud service consumers and cloud service providers. Cloud service providers offer access to their consumers using network and telecommunications technology. Internet-connected gadgets including desktops, notebooks, smartphones, tablets, and MIDs are examples of how cloud users might have access to these services. Most cloud services have their transit handled by network and communications companies. When discussing a company's ability to transfer data storage devices like high-capacity hard drives physically, the term "transport agent" is often used. A cloud provider can establish SLAs with a cloud carrier to ensure that the carrier's services are on track with the SLAs offered to cloud customers. The carrier can build secure, dedicated connections between cloud users and providers.

3.4 Basic Blocks of Cloud Computing:

The term "cloud computing architecture" describes the structure and parts of any cloud-based computer infrastructure. It is categorized into three Layers: Application Layer, Middleware layer, Application Layer. In a cloud system, both the Cloud Provider and the Cloud Consumer have access to and control over the system's resources. Application, middleware, and operating system layers make up the conventional software stack notation to illustrate these variations. The roles and duties of the various actors in cloud application management may be better grasped with this study of the division of controls over the application stack.

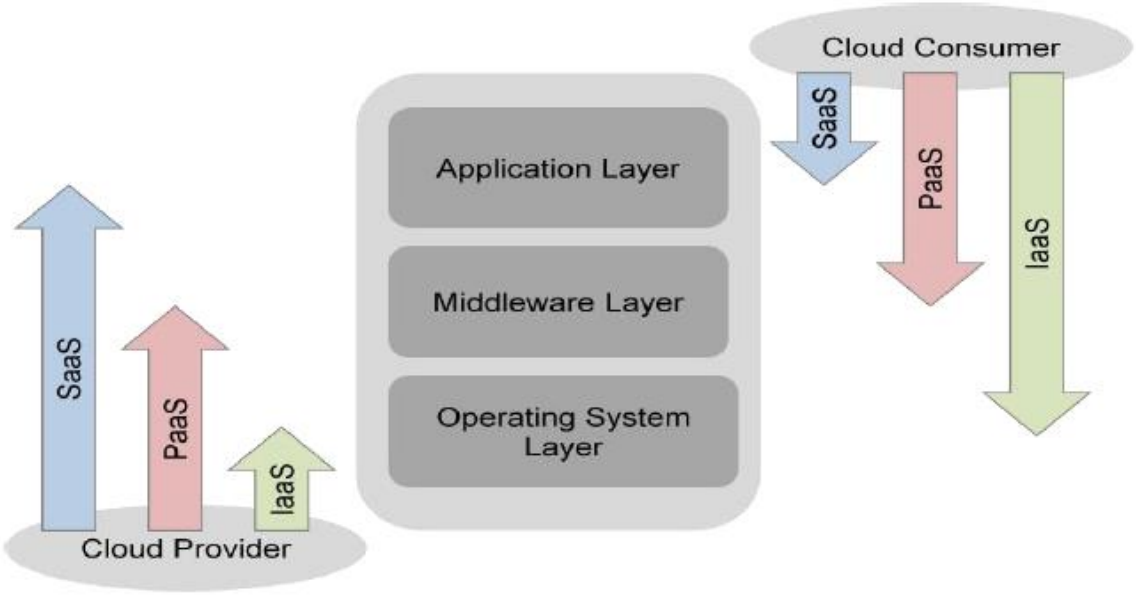

Figure 24 Layers in Cloud Computing [10]

- Applications that are designed for users or other machines at the application layer. Customers of PaaS, IaaS, and SaaS utilize the apps or pay the SaaS provider to set them up and take care of them.

- The middleware layer allows programmers to create cloud-based applications by providing the necessary software components (such as libraries, databases, and the Java virtual engine). Customers of Platform as a Service utilize the middleware, but neither they nor the suppliers of that service need to worry about installing, managing, or updating it.
- Customers of both SaaS and PaaS have no idea of the OS layer, which consists of the operating system and drivers. One or more guest operating systems can be virtualized and operate on a single physical host in an Infrastructure as a Service cloud. Customers often have a lot of flexibility in selecting a hosted operating system from among all the OS offered by the cloud service provider. In an IaaS model, the host operating system is managed by the provider, but the guest OS is the responsibility of the consumers.

3.5 Cloud Computing Deployment Models:

Cloud computing architecture can also be classified according to the deployment model. There are four types of deployment models:

- Private cloud
- Public cloud
- Hybrid cloud
- Community cloud

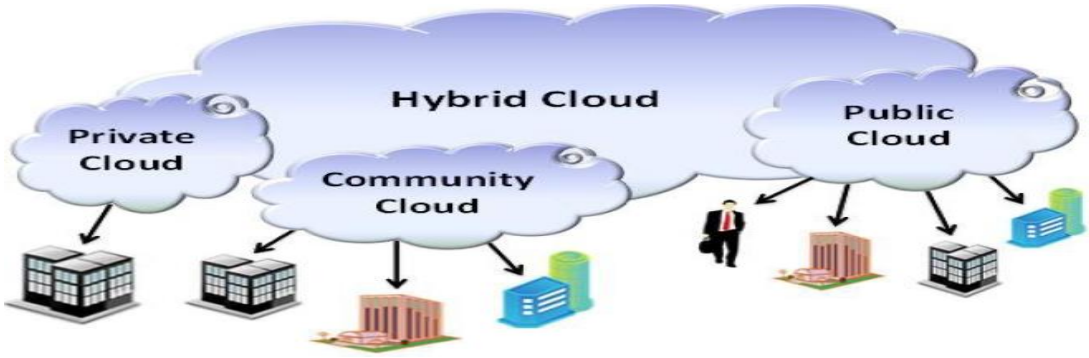

Figure 25 Cloud Computing Deployment Models [10]

3.5.1 Private Cloud:

The private cloud can be located in your company's data center or provided by an external supplier. However, with a private cloud, the hardware and software are reserved exclusively for your business, and the infrastructure is still controlled on a private network. The benefits of private clouds are listed below:

- **More flexibility:** This translates to the fact that companies are able to customize their cloud environments to meet their unique requirements.
- **High scalability:** Even private clouds provide users with the same scalability and operational efficiencies as public clouds.
- **Improved security:** Because resources are not made available to anybody else, it is feasible to achieve better levels of both control and security.

Information stored in a private repository is protected from being used by the broader public since only a select group of people can access it. Since there have been a lot of data breaches in recent years, many major companies have opted for the more secure closed private cloud model. Private clouds, as opposed to public ones, provide more autonomy in adapting the underlying infrastructure to the specific needs of each business. Businesses with mission-critical operations or rapidly evolving needs will find a private model to be the most beneficial.

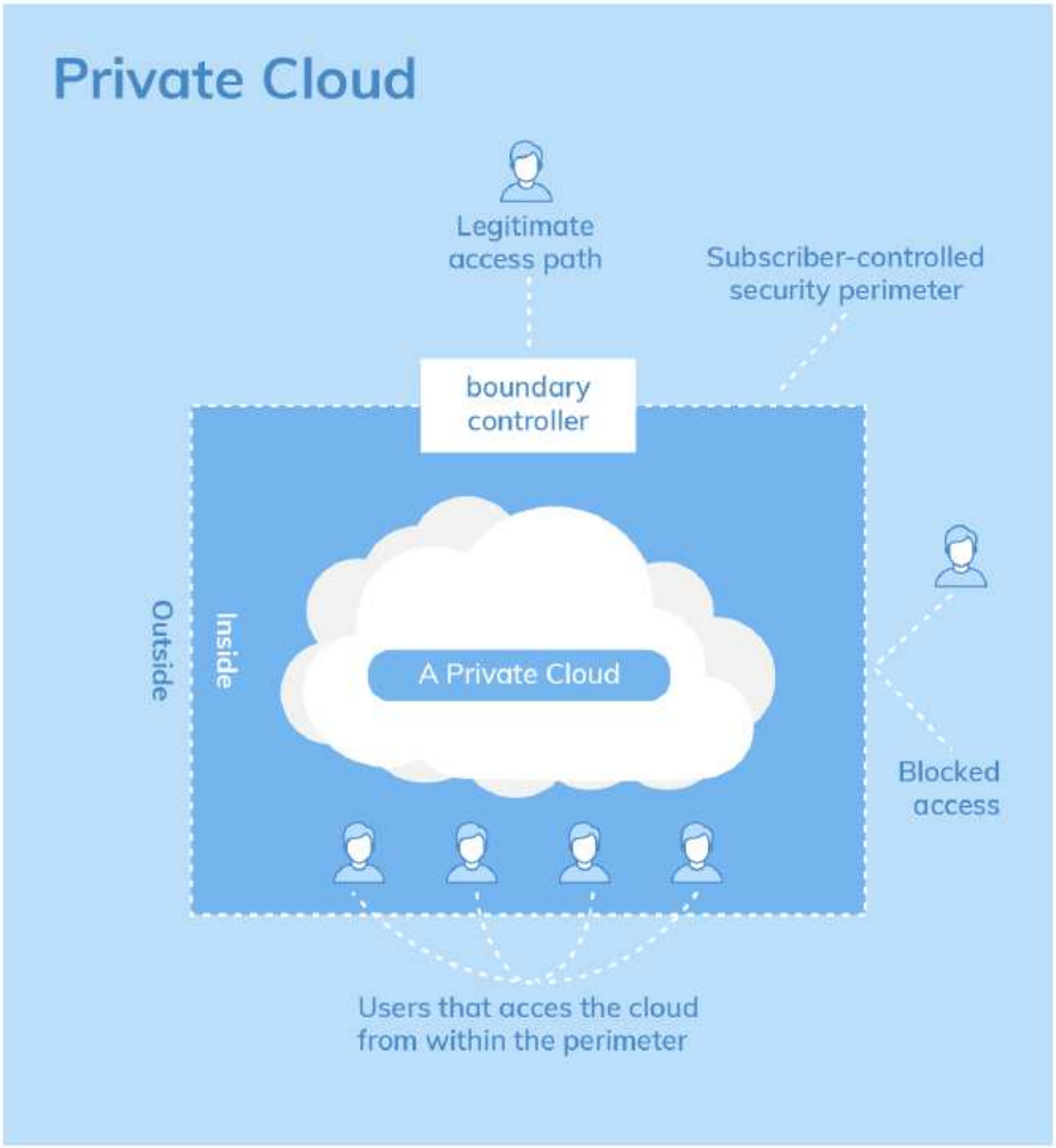

Figure 26 Private Cloud Deployment Model [10]

3.5.2 Public Cloud:

Using public clouds to implement cloud computing has proven to be the most common practice. The cloud services (including servers and storage) are managed and maintained by a third-party cloud service provider and made available through the Internet. Microsoft Azure is an example of a public cloud service. The public cloud's hardware, software, and underlying infrastructure are all owned and managed by the cloud provider. In a public cloud, you and other businesses (called "tenants") use the

same servers, data centers, and networks. You will use a web browser to access the services and control your account as a customer. The benefits of public cloud are :

- **Lower Cost:** You just need to pay for the service that you use, and there is no requirement to purchase any gear or software.
- **Unlimited Scalability:** There are resources accessible on demand that can cater to the requirements of your company.
- **No Maintenance:** Maintenance is an obligation that falls on the shoulders of the service providers.

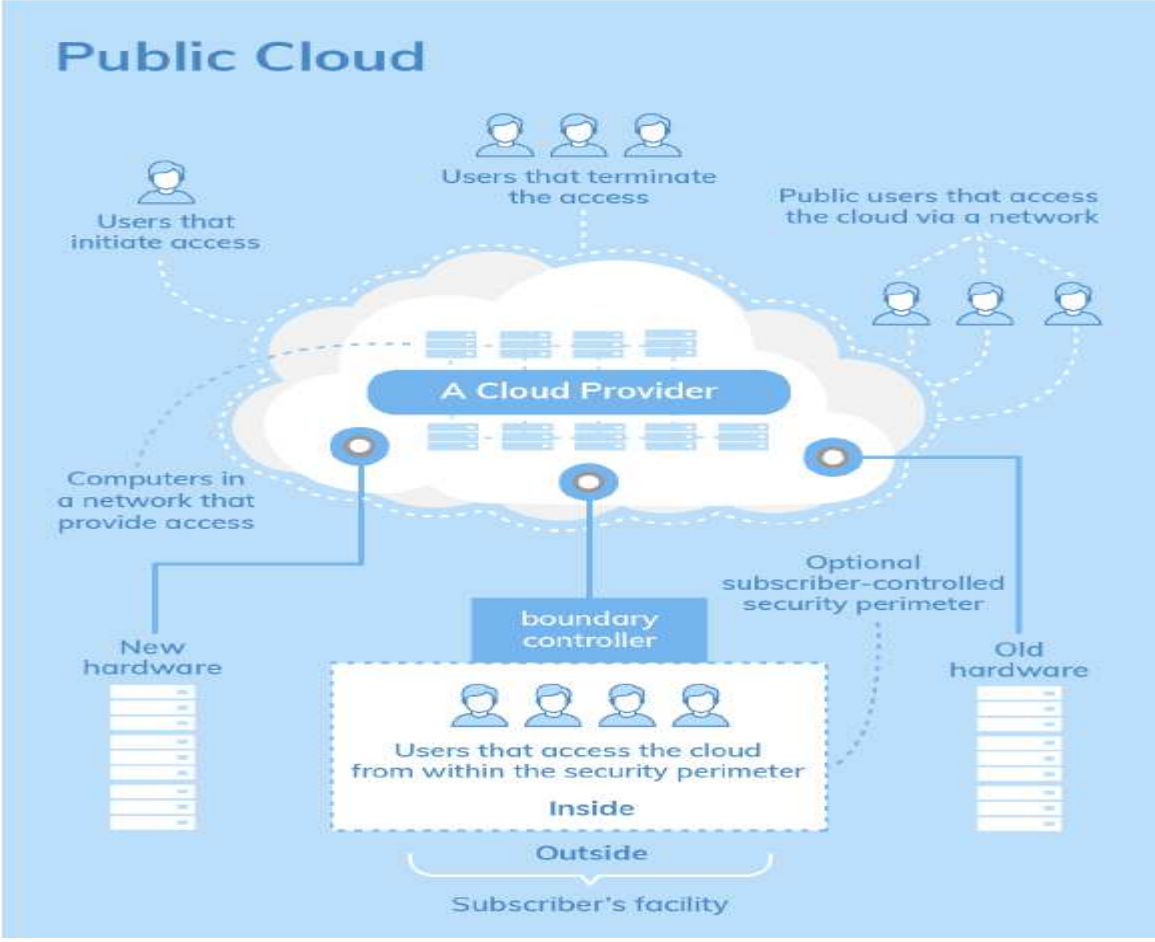

Figure 27 Public Cloud Deployment Model [10]

3.5.3 Hybrid Cloud:

The phrase "the best of both worlds" has been known to be used in reference to hybrid clouds. In other words, hybrid clouds blend private clouds with public clouds to allow businesses to reap the benefits of both types of clouds. By enabling the movement of data and applications between private and public clouds, hybrid cloud computing provides users with increased deployment options and flexibility. Depending on what you want, you can use either a private or public cloud. For instance, make use of the public cloud for high-volume applications requiring less protection, such as web-based email. However, the private cloud is the solution when it comes to sensitive company activities, such as financial reporting. The advantages of a Hybrid cloud are:

- **Flexibility:** This indicates that you may make use of the public cloud if you find yourself in need of additional resources.
- **Cost-effectiveness:** You just have to pay for the additional processing power that you need, and you may grow your resources on demand.
- **Control:** Your company is able to manage and monitor confidential infrastructure for application use.

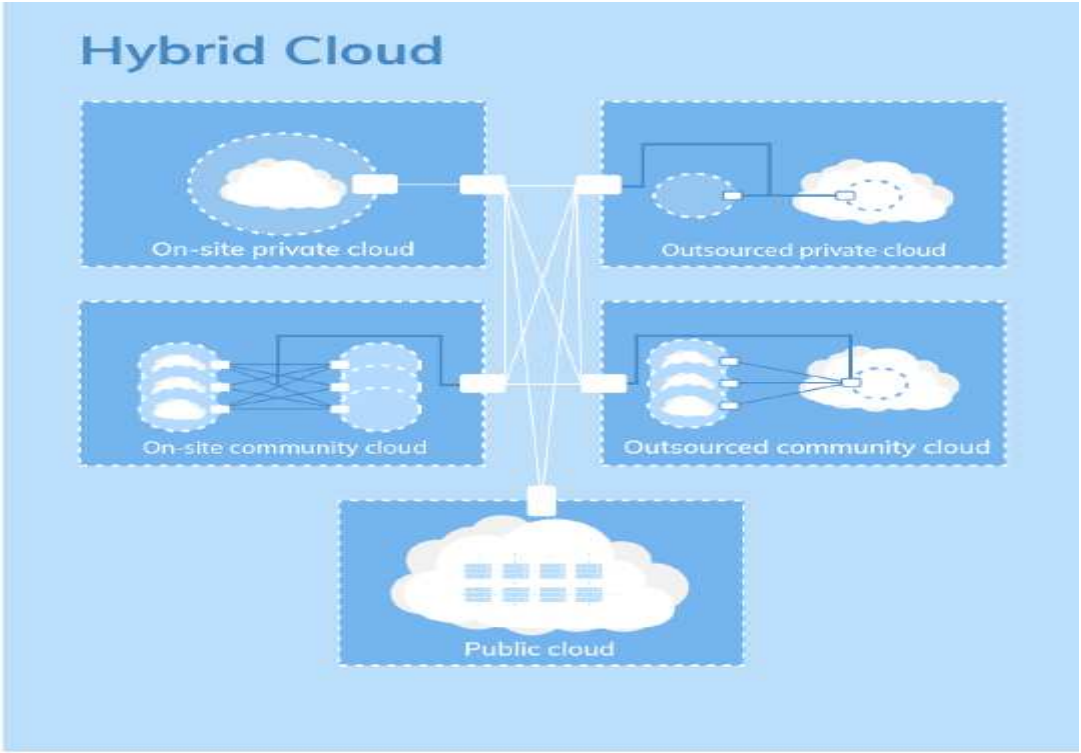

Figure 28 Hybrid Cloud Deployment Model [10]

3.5.4 Community Cloud: Community clouds are, in fact, decentralized systems that are constructed from a variety of cloud services and are designed to meet the unique demands that are imposed by communities or businesses. The users of a particular community cloud belong to a well-defined community that shares the same concerns or requirements; these users may be government entities, industries, or even simple individuals, but they all focus on the same issues while interacting with the cloud. This contrasts with public clouds, which cover several users simultaneously and may accommodate various services. On the other hand, private clouds offer services primarily to the company that is the cloud's owner. On the other hand, community clouds offer their services to the whole public. The advantages of Community cloud are:

- **No Failures:** Due to the fact that there is not a single service provider that is in charge of the infrastructure, there is no single point of failure.

- **Convenience and control:** Since a community cloud is both shared and managed by the community, which makes all of the choices through a collective democratic process, there is no conflict between the convenience of the cloud and the control that users have over it inside a community cloud.
- **Community:** The infrastructure is more scalable due to the fact that it is built on a collective that provides resources and services. This allows the system to grow by simply increasing the number of people that utilise it.

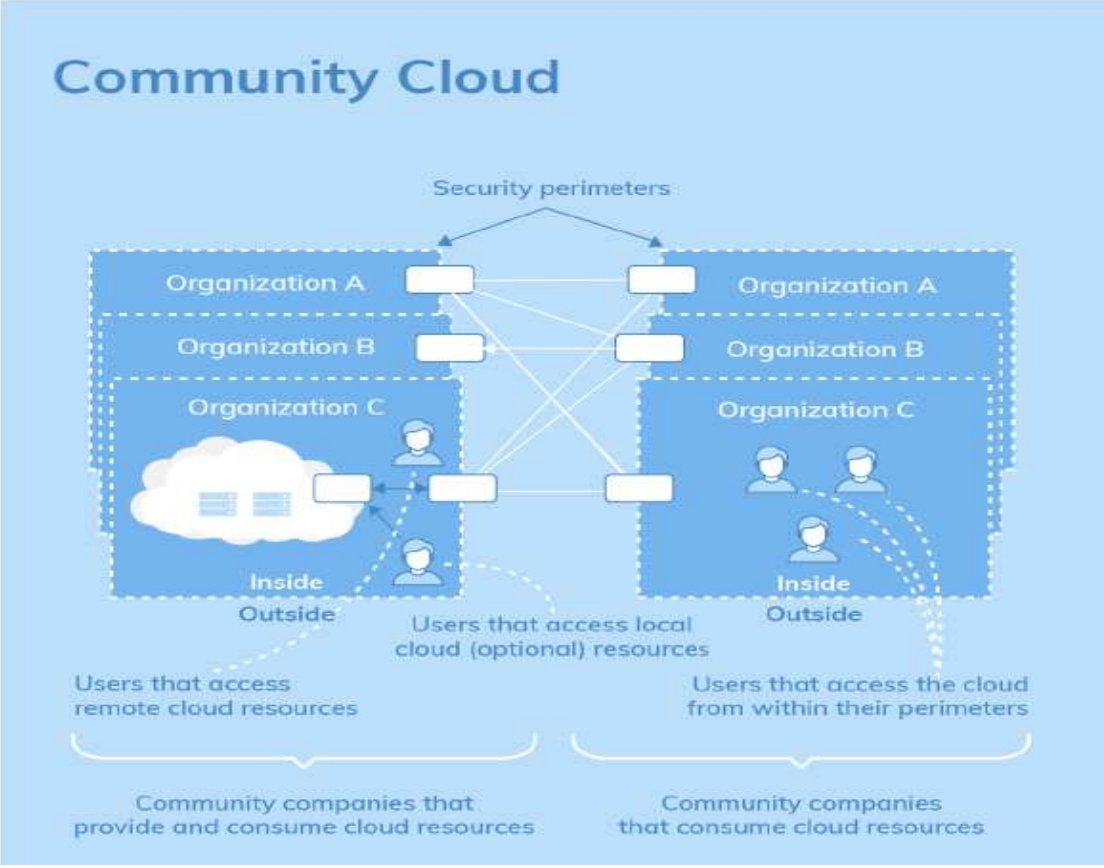

Figure 29 Community Cloud Deployment Model [10]

3.6 Security in Cloud Computing:

Cloud computing raises several significant problems, the most important of which are security (including data security and integrity, network security), privacy (including data secrecy), and service-level agreements. Due to the way resources are split across multiple cloud regions, data privacy and security are more likely to be breached. This causes enterprises to be more concerned about their sensitive data because of the increased risk of compromise.

The fact that cloud computing system typically offers services (such as DaaS, SaaS, IPMaaS, and PaaS, amongst others) to their users on the other side of the Internet. This means that the confidential information of individual users and companies is stored and handled by the service providers, which contributes to privacy issues. Concerns about users' privacy have been discussed in the computer literature for a long time, and various laws have been passed and published to protect users' personal privacy and the confidentiality of trade secrets. Three cloud service models (SaaS, PaaS, and IaaS) not only give specific services to end users but also reveal information security vulnerabilities and hazards of cloud computing systems.

Firstly, hackers might leverage the powerful computational capabilities given by clouds for malicious purposes. The most powerful features of a cloud are delivered directly via the lowest layer, where IaaS resides. Using it, users may create a "realistic" environment where many virtual computers coexist, each with its operating system. A hacker may rent a virtual machine, examine its setup and vulnerabilities, and then use that knowledge to launch an attack on other customers' virtual machines in the same cloud. IaaS also allows hackers to launch resource-intensive assaults like brute-force cracking. IaaS is attractive

to cybercriminals because it enables them to undertake assaults (such as distributed denial of service (DDoS) attacks) that need a large number of attacking instances.

Secondly, a significant vulnerability of cloud models is the potential for data loss. Businesses adopt SaaS cloud models to manage corporate information and customer records in the cloud. Programmers use data during the SDLC to ensure software security in PaaS cloud models (SDLC). To store information, users of IaaS cloud models build new drives on virtual computers. However, data in any of the three cloud types can be accessed by malicious insiders or outsiders. Data is vulnerable to purposeful or accidental access by inside staff. Many different forms of hacking, such as session hijacking and network channel eavesdropping, are used by external hackers to get access to databases in cloud systems.

Finally, the three levels of cloud systems are vulnerable to the same kinds of attacks that have been used against traditional networks. Authentication, authorization, and accounting flaws in the cloud can be exploited through many methods, such as web browser assaults. Viruses and Trojans are only examples of malicious software that may be deployed to cloud servers and create havoc.

It is crucial for businesses to be aware of the potential cyber security risks associated with cloud computing and to take measures to reduce those risks. Cloud computing can be subject to several cyber security attacks. The following are some concrete instances of potential cybersecurity risks posed by cloud computing:

3.6.1 Data Breaches:

When unauthorized people or organizations get access to sensitive data that is kept in the cloud, a data breach happens. Cloud computing may be used to store data. Cloud-based systems have the potential to be susceptible to hacking and other types of data

breaches, any of which can result in the loss of sensitive data or its theft. This can comprise a person's personal information, as well as their financial and intellectual property. The encryption of data, while it is at rest and in transit, should be implemented as an effective security measure in organizations. These security holes can appear for a variety of different reasons, including the following:

- Weak Security
- Insider threats
- Malware and ransomware
- Lack of encryption
- Unsecured API’s

Users and cloud providers must put in place rigorous security precautions to keep their data from being compromised. This involves the use of encryption, the implementation of multi-factor authentication, the routine patching and upgrading of systems, and the frequent performance of security audits and vulnerability assessments.

3.6.2 Denial-of-service (DoS) attacks:

DoS attacks, which can disrupt service and render apps and resources inaccessible to users, can be launched against cloud-based systems as a target. These kinds of assaults can be carried out by flooding a system with excessive traffic or by taking advantage of weaknesses in the system's underlying architecture. Organizations must use DDoS protection services to check that their computer networks are set up to deal with enormous traffic loads. There are different types of DoS attacks, like Distributed Denial of Service (DDoS) attacks, where the attacker uses multiple devices to generate traffic to the target.

Cloud providers and end users have a number of options at their disposal for preventing denial-of-service (DoS) assaults. Cloud computing service providers and end users alike have a number of defence mechanisms at their disposal to ward against denial-of-service assaults, including the following:

- Firewall to filter unwanted traffic
- Using traffic shaping to limit the amount of traffic that can be directed at a service
- Implementing rate limiting to block traffic that exceeds a certain threshold
- Using cloud-based DDoS protection services
- Having a response plan in place to quickly identify and mitigate a DoS attack.

It's vital to protect yourself from DoS assaults to keep up with the current threats and best practises, as these attacks are always changing and developing new tactics.

3.6.3 Malware based attacks:

Malware threatens cloud-based systems because it can compromise data security and cause service interruptions. Email, compromised websites, and harmful programs are all potential vectors for the spread of malware. To identify and respond to malware infestations, businesses should deploy anti-malware software and do frequent vulnerability assessments.

3.6.4 Phishing:

Cloud users can fall victim to phishing attacks, which can trick them into providing sensitive information or clicking on malicious links. Phishing attacks can be delivered via email, social media, or other communication channels. Organizations should educate employees about the dangers of phishing and provide them with tools and guidance to identify and report phishing attempts.

3.6.5 Insider threats:

Cloud-based systems can be vulnerable to insider threats, such as employees who misuse their access to sensitive information. This can include employees who steal data or disrupt service, or those who unknowingly compromise security through poor security practices. Organizations should implement access controls and monitoring systems to detect and respond to insider threats.

3.6.6 Account or Service Hijacking:

Attackers could gain unauthorized access to cloud service accounts or steal credentials, allowing them to compromise or disrupt services. This can be done through phishing, social engineering, or exploiting vulnerabilities in an organization's IT environment. Organizations should use multi-factor authentication and regularly review and update user access controls

3.6.7 Inadequate security controls:

Cloud-based systems can be vulnerable if security controls are not properly configured or implemented. This can include misconfigured firewalls, unpatched systems, or weak passwords. Organizations should conduct regular security assessments and audits to ensure their systems are properly configured and secure.

3.6.8 Compliance:

Cloud-based systems can be vulnerable to non-compliance with regulatory requirements regarding data protection and privacy. Organizations should ensure that their cloud-based systems comply with relevant laws and regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

4 Introduction to Edge Computing:

The concept of edge computing is another paradigm that improves the handling, storage, and processing of data created by networked devices. In contrast to traditional cloud computing, edge computing operates at the very edge of the network, just a hop away from individual IoT devices. As defined by OpenEdge Computing, Edge computing is carried out by decentralized nodes located near end users or at the network's periphery.

The original goal of edge computing was to provide ease of access to computing and storage resources in a secure environment near the user. Edge computing architecture is designed to reduce latency, improve scalability, and increase data privacy by enabling data processing to occur closer to the source of data generation.

The need for edge computing has arisen due to the increasing number of connected devices, known as the Internet of Things (IoT), and the growing volume of data generated by these devices. With billions of connected devices expected to generate data in the coming years, centralized data centers and cloud computing solutions need help to keep up with the demands of processing this data in realtime. This has led to the emergence of edge computing as a solution to address these challenges.

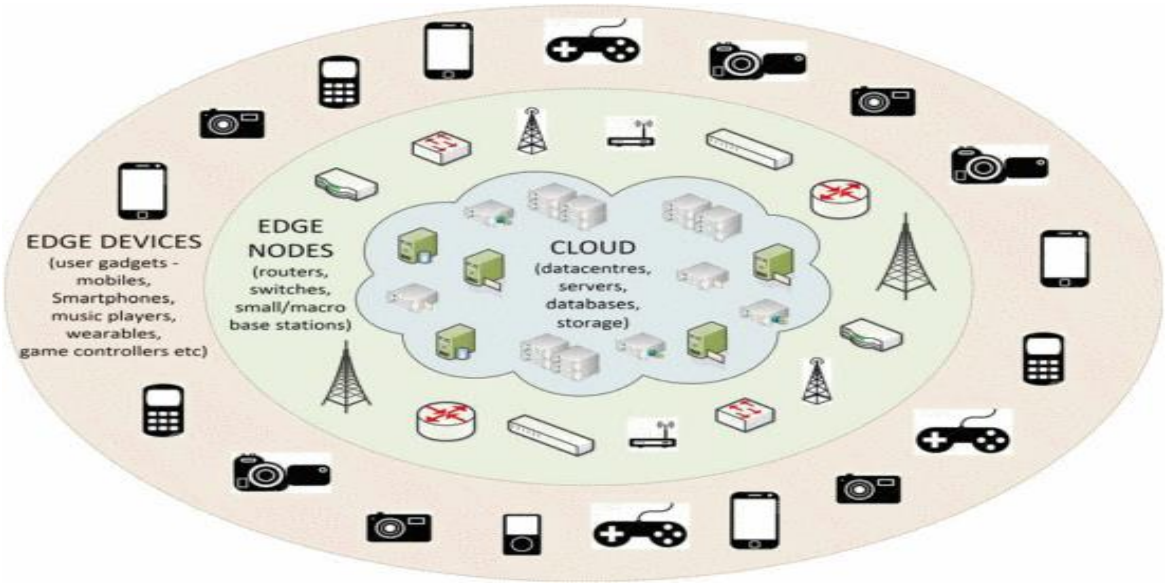

Figure 30 Various Devices connected to Data center through Edge nodes [11]

Edge computing is used for various industries and scenarios, including manufacturing, retail, transportation, and healthcare. In manufacturing, edge computing can process data from machines and sensors in real-time, enabling predictive maintenance and improved operational efficiency. In the retail industry, edge computing can process customer data, such as purchase history, to offer personalized recommendations and targeted advertising. In the transportation industry, edge computing can process data from connected vehicles, enabling real-time traffic analysis and routing optimization. In the healthcare industry, edge computing can process medical data from wearable devices and medical equipment, enabling real-time monitoring and analysis of patient data.

In other words, the edge is the immediate first hop, such as WiFi access points or gateways, from the IoT devices (not the IoT nodes themselves). This computational paradigm is known as edge computing if it is performed on IoT devices. General Electric states that edge computing focuses on edge device interactions (e.g., RANs, base stations, or edge routers). Edge computing solutions can be deployed on various devices, including routers, switches, and embedded systems. Edge gateways act as intermediaries between the edge devices and the cloud, enabling data to be processed and transmitted in real-time. Edge routers and switches route data between edge devices and the cloud. In contrast, embedded systems perform computation and data processing on the edge devices themselves.

4.1 Need of Edge Computing:

- Data processing on the cloud is effective because the cloud's computational capability exceeds the edge's. However, data processing speed is outpacing network bandwidth. Data transmission speed limits cloud-based computing as edge data production increases. For instance, a Boeing 787 can generate five terabytes of data per second, but the bandwidth between the aircraft and the

ground-based satellite or base station is too low to transfer data. The cloud will take too long to process all the data. Its ability to handle several automobiles in one place will strain network bandwidth and dependability. Data should be handled at the edge for faster response time, better processing, and lower network stress.

- Almost all kinds of electrical devices, like air quality sensors, LED bars, streetlights, and even microwave ovens connected to the Internet, will be a part of the IoT. These devices will create and use data, like sensors for measuring air quality, LED bars, and streetlights. In a few years, the number of devices in the network's periphery will increase to over a billions. In other words, most data created by IoT devices will never make its way to the cloud and will instead be used by end users at the network's periphery.
- Cloud computing's edge devices often consume data, such as when you watch a YouTube video on your smartphone. People still create data from their mobile devices nowadays. The move from data user to data producer/consumer requires more edge function placement. Today, individuals capture photos and videos and upload them to YouTube, Facebook, Twitter, or Instagram. YouTube uploads 72 hours of new video material per minute, Facebook shares roughly 2.5 million pieces of content, Twitter tweets almost 300,000 times, and Instagram posts almost 220,000 new photographs. Uploading the photo or video may need a lot of bandwidth. Instead, the video clip should be reduced and converted to the necessary resolution at the edge before being uploaded to the cloud.
- Due to all these reasons edge computing is needed more then ever to streamline the networks and clouds.

4.2 Attributes of Edge Computing:

Some of the key benefits of edge computing are:

- **Lower Latency:** One of the critical benefits of edge computing is its ability to reduce latency. By processing data at the network's edge, edge computing solutions can reduce the time it takes for data to be transmitted to a central data center or cloud, enabling real-time data processing and decision-making. This can be particularly important in industries such as transportation, where real-time data processing is critical for ensuring the safety of passengers and optimizing traffic flow. In today's world, latency is a crucial aspect of the gaming domain.
- **Improved Bandwidth Efficienc**y: The quantity of data that has to be transferred over the network can be reduced due to edge computing, which helps to increase bandwidth efficiency and therefore cut expenses.
- **Better Data Privacy:** Edge computing solutions can limit the quantity of data transferred to the cloud by processing data at the network's edge. This, in turn, reduces the risk of data breaches and unauthorized access to critical information. This can be of uttermost significance in sectors such as the healthcare industry, where maintaining the confidentiality of patient information is of the utmost significance.
- **Increased Reliability:** Through the distribution of computing resources over a multitude of edge devices and a reduction in reliance on a single, centralized cloud, edge computing can improve the system's overall stability.
- **Enhanced Scalability:** Instead of depending on a centralized data center or the cloud, edge computing allows increased scalability by permitting data processing on the edge devices themselves. This eliminates the need for a third party to host the data. This can significantly reduce the quantity of data that has to be transferred to the

cloud, easing the load on network resources and contributing to an improvement in the system's overall performance.

- Edge computing is a method that brings computer resources closer to the consumers and devices that create and consume data. This can assist in enhancing the user experience, cutting costs, boosting dependability, and solving concerns about data privacy.

4.3 The link between Cloud Computing, IoT and Edge computing:

Cloud computing, IoT (Internet of Things), and edge computing are all interconnected technologies that work together to enable new applications and use cases in various industries. The link between these technologies can be described as follows.

- The Internet of Things generates an enormous quantity of data, which needs to be saved, processed, and evaluated in order to get any insights that are valuable.
- The infrastructure required to store and handle this data in a manner that is both cost-effective and scalable is made available by cloud computing. Additionally, it offers capabilities for sophisticated analytics and machine learning so that insights may be gleaned from the data.
- However, because of the high latency and bandwidth requirements, it may be impossible to transfer all of the data generated by IoT devices to the cloud. Edge computing solves this problem by moving the compute and storage closer to the Internet of Things devices and doing the data processing on a local level.

- Before sending the data to the cloud, edge computing may filter, preprocess, and aggregate it, which lowers the amount of data that is sent and the expenses associated with it.
- In a nutshell, cloud computing, the Internet of Things, and edge computing all collaborate to make real-time data processing, analysis, and decision-making possible. This is an important capability for a wide variety of applications, including smart homes, autonomous vehicles, industrial automation, and healthcare.

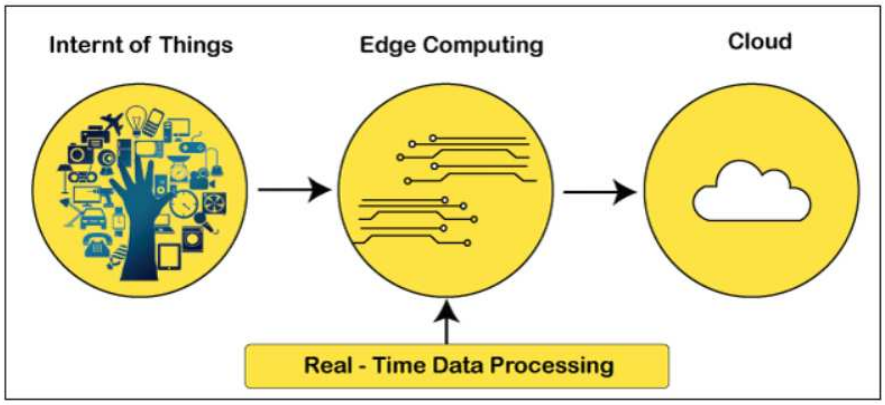

Figure 31 Interconnection between IoT, Cloud and Edge Computing [11]

4.4 Architecture of Edge Computing:

Many different Edge computing architectural models can be found, but, the most commonly used is based on three layered architectural model. The three layers of the edge computing architecture are Edge Device layer, Cloud Server Layer and Edge Server layer .These layers are discussed below.

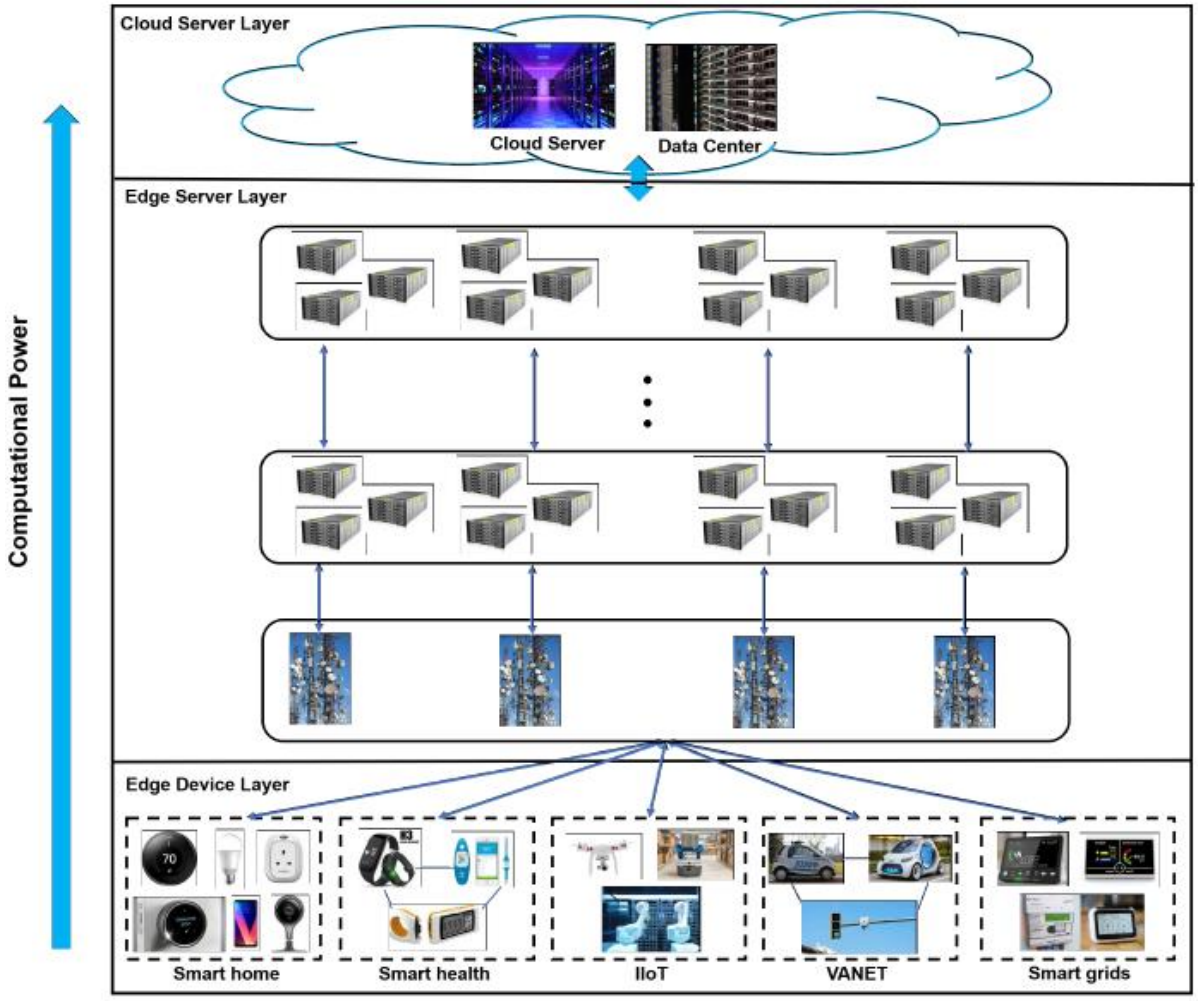

Figure 32 Edge Computing Architecture[12]

4.4.1 **Edge** Device **Layer:**

The edge layer in edge computing architecture refers to the devices and equipment located at the network's edge, close to where the data is generated. This includes various devices, such as sensors, cameras, smart devices, and other IoT devices deployed in various environments, including industrial, commercial, and residential settings.

The edge layer is critical in edge computing architectures as it generates the data that is processed, stored, and analyzed. This layer is responsible for capturing and

transmitting the data to other parts of the system, such as the fog or cloud computing layer, where it can be processed and analyzed.

The edge layer has a number of key features, including:

- **Resource Constraints:** Edge devices typically have limited processing, storage, and communication capabilities, so it's important that the edge layer is designed to operate effectively in these resource-constrained environments .
- **Autonomy:** Edge devices are often deployed in remote or difficult-to-reach locations, so it's important that they can operate autonomously and make local decisions without the need for continuous communication with the central data center.
- **Security:** Edge devices can be vulnerable to security threats, so the edge layer must be designed to be secure, with appropriate security measures in place to protect the devices and the data they generate.

In conclusion, the edge layer is the foundation of edge computing architecture, providing the devices and equipment that generate the data that is processed, stored, and analyzed in other parts of the system. The edge layer has key features, including resource constraints, autonomy, and security, that must be considered when designing and deploying edge computing solutions

4.4.2 Edge server Layer:

This layer in edge computing architecture refers to a layer of computing resources that lies between the edge devices and the central data center. It acts as an intermediary between the edge devices and the central data center, providing processing, storage, and communication capabilities closer to the edge of the network.

The fog layer is designed to address the challenges posed by traditional centralized computing models, where the central data center is responsible for

processing and storing all the data generated by the edge devices. This approach can lead to network congestion, high latency, and limited scalability, especially in IoT environments where the number of edge devices is growing rapidly.

The fog layer provides a distributed computing environment that can process and store data closer to the edge devices, reducing the amount of data that needs to be sent to the central data center. This can reduce latency, improve response times, and increase the reliability and efficiency of the system.

The fog layer can also provide a range of other benefits, such as:

- **Data Filtering and Aggregation:** The fog layer can perform data filtering and aggregation functions, reducing the data that needs to be sent to the central data center. This can help to reduce network congestion and improve the efficiency of the system.
- **Local Processing and Decision-Making:** The fog layer can perform local processing and decision-making functions, reducing the data that needs to be sent to the central data center. This can improve the efficiency and reliability of the system and reduce the risk of network congestion.
- **Security:** The fog layer can provide a range of security functions, such as encryption and data anonymization, to protect sensitive data and ensure the privacy of users.

The fog layer is an essential component of the edge computing architecture that provides processing, storage, and communication capabilities closer to the edge of the network. It offers a range of benefits, including reduced latency, improved reliability, increased efficiency, and enhanced security, making it an important part of any edge computing solution.

4.4.3 Cloud Server Layer:

Cloud Server layer in edge computing architecture refers to the central data center or cloud-based infrastructure that provides a range of computing, storage, and communication services over the internet. The cloud computing layer is typically used in edge computing architectures to provide a centralized repository for data generated by edge devices and to perform centralized processing and analysis of this data.

The cloud computing layer is a key component of edge computing architectures as it provides a centralized environment for data storage and management, which is essential for large-scale edge computing deployments. The cloud computing layer can store and manage large amounts of data generated by edge devices and provide a range of processing and analytics services, such as machine learning and big data analytics, to extract value from this data.

In addition, the cloud computing layer provides a range of benefits, including:

- **Scalability:** The cloud computing layer is highly scalable, allowing organizations to add and remove computing resources as needed, to meet changing demands.
- **Flexibility:** The cloud computing layer provides a flexible and on-demand infrastructure, allowing organizations to quickly and easily deploy new applications and services.
- **Cost-effectiveness:** The cloud computing layer provides cost-effective computing and storage resources, allowing organizations to reduce their capital and operational expenses.

The cloud computing layer is an important component of edge computing architecture, providing a centralized repository for data storage and management and a range of processing and analytics services.

4.5 Applications of Edge Computing:

The following is a list of some of the potential applications that may be developed using edge computing:

4.5.1 Cloud Offloading:

Cloud offloading in edge computing refers to transferring processing and storage tasks from the central data center to the edge devices. This is typically done to reduce the amount of data that needs to be transmitted over the network to the central data center, improving the performance and efficiency of the system.

Cloud offloading can be performed in many ways, including:

- **Task offloading:** This refers to the transfer of specific processing tasks from the central data center to the edge devices, allowing the edge devices to perform the tasks locally and reducing the need for data transmission over the network.
- **Data offloading:** This refers to the transfer of data from edge devices to the central data center, where it can be stored and processed. Data offloading can reduce the storage and processing requirements at the edge, improving overall system performance and efficiency.
- **Hybrid offloading:** This refers to a combination of task and data offloading, where both processing tasks and data are transferred from the central data center to the edge devices, depending on the application's specific requirements.

4.5.2 Smart Cities:

Edge computing is utilised in the application of smart cities to enable real-time monitoring and control of municipal infrastructure, such as the administration of public safety, energy management, and transportation. In smart cities edge computing is used to handle larger data quantity, low latency issues and location management.

4.5.3 Smart Homes:

IoT and edge computing have improved home environments recently. Smart TVs, lights, and vacuums are available on the market. However, more than connecting a Wi-Fi module to the electrical unit and the cloud is required for a smart house. In a smart house, affordable wireless sensors and controllers should be installed in the room, pipe, floor, and wall in addition to the linked device.

These things will report a lot of data, which should be consumed at home for data transportation pressure and privacy protection. This renders cloud computing inappropriate for smart homes. However, edge computing is suitable for creating a smart home: with an edge gateway running an edge operating system (edgeOS) in the home, stuff can be easily linked and handled, data can be processed locally to relieve Internet bandwidth, and the service can be installed on the edgeOS for better management and distribution.

4.5.4 Industrial Automation:

In the field of industrial automation, edge computing is utilised to enable real-time monitoring and management of production processes. This results in increased levels of both efficiency and productivity.

4.5.5 Healthcare:

In the healthcare industry, edge computing is utilised to provide real-time monitoring of patients and medical devices, which enables enhanced patient care and results. Edge computing offers a wide range of applications across a variety of business sectors since it enables the real-time processing and analysis of data provided by edge devices. This enables businesses to increase their efficiency and productivity, as well as the quality of the services and experiences they deliver to their clients, as well as make more informed decisions.

4.6 Challenges in Edge Computing:

Edge computing is a relatively new technology and as such, it faces several challenges that need to be addressed in order to realize its full potential. This technology enables low latency and high bandwidth data processing, making it ideal for use cases such as real-time streaming, autonomous vehicles, industrial IoT, and more. However, despite its advantages, edge computing also faces several challenges that must be addressed to ensure its success. Some of the key challenges in edge computing include:

1. **Latency and Bandwidth Constraints:** One of the main challenges of edge computing is the need to process large amounts of data in real-time, with low latency and high bandwidth. Edge devices are often connected to the network via wireless connections, which can be subject to interference, network congestion, and other factors that can negatively impact performance. To overcome these challenges, edge computing systems must be optimized for low latency and high bandwidth.
2. **Security:** Edge computing devices are often connected to the network via wireless connections, making them vulnerable to cyber threats such as hacking, malware, and other forms of malicious activity. To ensure the security of edge computing systems,

it is necessary to implement strong security measures such as encryption, authentication, and firewalls.

3. **Interoperability:** Edge computing systems are often deployed across multiple devices and networks, making it necessary to ensure that they are interoperable with each other. This requires the development of common standards and protocols that can be adopted across different vendors and systems.
4. **Scalability:** Edge computing systems must be able to scale to meet the growing demand for data processing and storage. This requires the development of scalable architectures and systems that can support large amounts of data and processing power.
5. **Energy Efficiency:** Edge computing systems must be designed to be energy efficient, as they are often deployed in remote locations and may not have access to reliable power sources. This requires the development of low-power devices and systems that can operate for extended periods without requiring frequent recharging.
6. **Cost:** Edge computing systems must be cost-effective, as they are often deployed in large numbers and in remote locations. This requires the development of low-cost devices and systems that can be deployed and maintained at scale.
7. **Data Management:** Edge computing systems must be able to effectively manage the large amounts of data generated by connected devices. This requires the development of effective data management strategies and systems that can handle data storage, processing, and analysis.
8. **Compliance:** Edge computing systems must be compliant with relevant regulations and standards, such as data privacy regulations, data security standards, and industry-specific standards. This requires the development of systems that are designed with compliance in mind and are capable of meeting these requirements.

9. **Reliability:** Edge computing systems must be reliable, as they are often deployed in critical applications where downtime is not an option. This requires the development of systems that are robust and able to operate in harsh environments.
10. **Maintenance:** Edge computing systems must be easy to maintain, as they are often deployed in remote locations and may not have access to on-site support. This requires the development of systems that are designed for ease of maintenance and can be easily repaired and updated.

Edge computing has the potential to transform a range of industries and applications. However, to achieve its full potential, it is necessary to overcome the challenges discussed above. This will require collaboration and investment from industry, government, and academia to develop systems that are secure, scalable, and cost-effective, and that meet the needs of users. By addressing these challenges, edge computing has the potential to revolutionize the way we process, store, and analyze data, enabling new applications and use cases that were previously not possible.

4.7 Cybersecurity attacks/threats and their mitigation in Edge Computing:

1. Man-in-the-Middle (MITM) Attacks:

A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts the communication between two parties. In edge computing, the attacker can intercept the communication between the edge devices and the central computing systems, allowing them to modify or steal sensitive information. MITM attacks can occur in a lots of ways, such as through unencrypted communications, fake Wi-Fi hotspots, or by compromising the network infrastructure.

Prevention: To prevent MITM attacks, it is recommended to implement encryption for all communication between edge devices and the central computing systems. Additionally, the use of secure protocols, such as SSL/TLS, can help to prevent attackers

from intercepting and altering the communication. It is also important to ensure that all Wi-Fi hotspots and network infrastructure components are properly secured and configured.

2. **Denial of Service (DoS) Attacks:**

A Denial of Service (DoS) attack occurs when an attacker floods a network with a large amount of traffic, effectively rendering it unavailable to legitimate users. In edge computing, DoS attacks can occur at various levels, such as at the device, network, or cloud level.

Prevention: To prevent DoS attacks in edge computing, it is recommended to implement network security measures such as firewalls and intrusion detection systems. Additionally, implementing rate limiting and traffic filtering can help to prevent attackers from overwhelming the network or system with traffic.

3. **Remote Code Execution (RCE) Attacks:**

Remote Code Execution (RCE) attacks occur when an attacker executes arbitrary code on a remote system. In edge computing, RCE attacks can occur through vulnerabilities in the software running on edge devices or in the central computing systems.

Prevention: To prevent RCE attacks, it is important to ensure that all software used in the edge computing infrastructure is kept up-to-date and patched to eliminate any known vulnerabilities. Additionally, implementing network segmentation and access control measures can help to restrict the potential attack surface and limit the impact of an RCE attack.

4. **Data Leakage:**

Data leakage occurs when sensitive information is accidentally or intentionally disclosed to unauthorized parties. In edge computing, data leakage can occur through a variety of mechanisms, such as through unencrypted communications, device theft, or employee error.

Prevention: To prevent data leakage in edge computing, it is important to implement encryption for all sensitive information, both in transit and at rest. Additionally, implementing access control measures, such as role-based access control and multi-factor authentication, can help to make ensure that only authorized personnel have access to sensitive information.

5. **Insider Threats:**

Insider threats refer to threats that originate from within an organization, such as through employee error or malicious activity. In edge computing, insider threats can occur through a variety of mechanisms, such as through unauthorized access to sensitive information or the compromise of edge devices.

Prevention: To prevent insider threats in edge computing, it is important to implement strict access control measures, such as role-based access control and multi-factor authentication, to limit the access to sensitive information to only those who need it. Additionally, regular security awareness training can help to educate employees on the importance of maintaining secure practices and reduce the risk of accidental security breaches.

6. **Physical Theft or Tampering of Edge Devices:**

Edge devices are often located in physically accessible locations, making them vulnerable to theft or tampering. This can result in the loss or theft of sensitive information, as well as the compromise of the device itself.

Prevention: To prevent physical theft or tampering of edge devices, it is important to implement physical security measures such as secure enclosures, locks, and surveillance cameras. Additionally, implementing remote device management and remote wipe capabilities can help to ensure that sensitive information is protected in the event of a device theft or tampering. Regular audits and inspections of edge devices can also help to detect and prevent any unauthorized access or tampering.

7. **Unsecured Connections to the Cloud:**

Edge computing often involves transmitting data to and from the cloud, making it vulnerable to attacks on the communication channels. Unsecured connections can result in the interception or alteration of sensitive information.

Prevention: To prevent unsecured connections to the cloud, it is important to implement encryption for all communication between edge devices and the cloud. Additionally, implementing secure protocols such as SSL/TLS can help to prevent attackers from intercepting or altering the communication. Regular security assessments and audits can also help to detect any vulnerabilities in the communication channels.

8. **Rogue Edge Devices:**

Rogue edge devices refer to edge devices that are not properly secured or managed, and can potentially compromise the security of the entire edge computing infrastructure. These devices may be the result of poor device management practices, or maybe maliciously introduced into the network.

Prevention: To prevent rogue edge devices, it is important to implement strict device management practices, such as regular audits and inspections of edge devices, and secure device configurations. Implementing network segmentation and access control measures can also help to limit the potential attack surface and prevent rogue edge devices from compromising the security of the entire network.

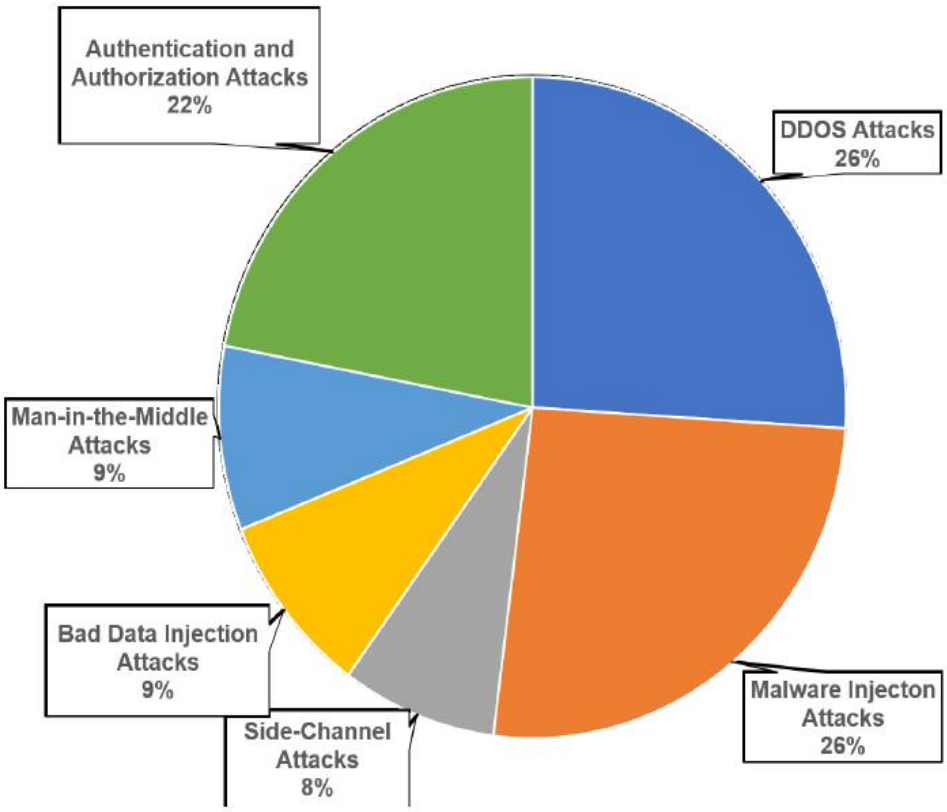

Figure 33 Show Percentage of attacks on Edge Computing[12]

5 DDOS Attacks:

A Distributed Denial of Service (DDOS) attack is a type of cyber attack that aims to overload a target system with a large volume of traffic, making it unavailable to legitimate users. This type of attack is particularly devastating in edge computing systems, as the decentralization of these systems can make it easier for attackers to launch a coordinated attack from multiple points. DDOS attacks can result in operational disruptions, causing websites, applications, and systems to become unavailable to legitimate users. This can result in lost business, as customers may be unable to access the products and services they need. DDOS attacks can also cause reputational damage,

as customers may view the organization as unreliable if its systems are frequently unavailable.

Prevention: To prevent DDOS attacks, organizations should implement strong network security measures, such as firewalls and intrusion detection systems. They should also use traffic filtering and rate-limiting technologies to limit the amount of traffic that can reach their systems. Additionally, organizations should use content delivery networks (CDNs) or Software delivered Networks (SDNs) to distribute their traffic across multiple locations, making it more difficult for attackers to overload a single point of failure.

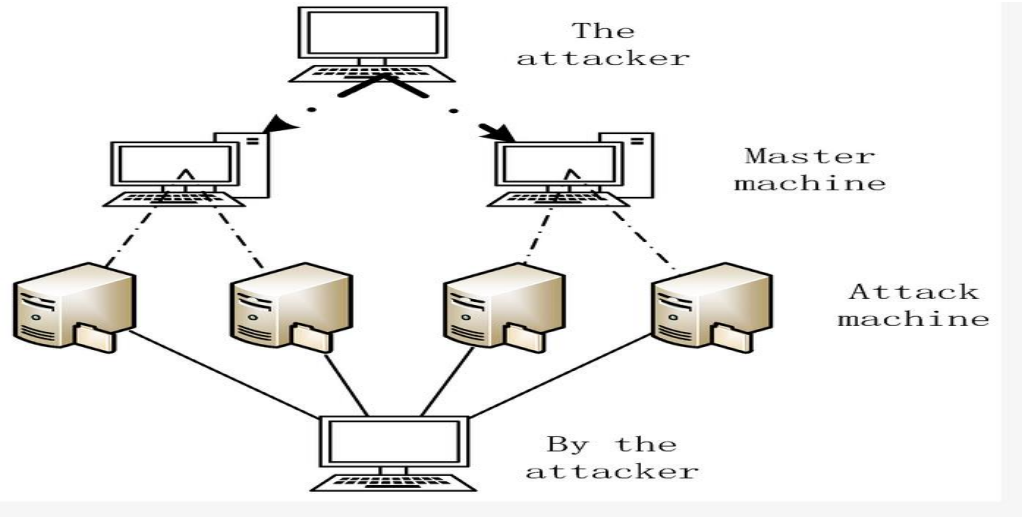

Figure 34 Schematic Illustration of DDOS attack (Source: Google images)

Some use cases of DDOS attack in edge computing are:

1. **Targeting Industrial Control Systems (ICS):** Industrial control system (ICS) networks in edge computing are vulnerable to DDOS assaults, which can halt manufacturing lines, power grids, and water purification systems. This kind of attack can have serious effects, such as financial losses, safety risks, and damage to the environment.
2. **Interfering with Autonomous Systems:** Self-driving vehicles and drones are only two examples of autonomous technologies that are vulnerable to DDOS assaults that

might cause them to malfunction or even crash. There's a risk of harm and property damage as a result.

3. **Disrupting Emergency Services:** Computing at the network's edge is used by emergency responders to relay time-sensitive data and geolocation coordinates from vehicles like ambulances and fire engines. At emergency scenarios, people's lives may be in jeopardy if communication and reaction times were slowed by DDOS assaults on these systems.
4. **Disrupting Smart City Services:** Applications of edge computing in smart cities include traffic control, public safety, and environmental monitoring. Essential services might be compromised by a DDOS assault on these networks, leading to widespread chaos and inconvenience for people.

   Firewalls, intrusion detection systems, and SDN-based traffic filtering are all important tools for protecting against distributed denial-of-service (DDOS) assaults in edge computing.In order to reduce the likelihood of being penetrated by DDOS assaults, it is also important to keep edge devices up-to-date with the latest security patches and software upgrades on a consistent basis.

5.1 Mitigations for DDOS attacks:

DDoS assaults are a sort of cyber-attack that can interrupt the regular operation of a server or network by overloading it with an excessive amount of traffic. Due to the dispersed infrastructure, edge computing, which includes processing data closer to the source of the data, is susceptible to DDoS assaults. Here are some potential DDoS attack mitigation techniques for edge computing.

- **Traffic filtering:** Filtering away malicious traffic is one of the most frequent defences against distributed denial of service attacks (DDoS). When it comes to preventing harmful traffic from reaching the core infrastructure, edge computing

nodes can utilise firewalls and intrusion prevention systems to identify and stop it before it even gets there.

- **Resource provisioning:** By scaling up their capacity, edge computing systems may be configured to deal with the additional traffic that occurs during DDoS assaults. This can be accomplished through the use of strategies that include dynamic resource allocation, as well as by the addition of more processing power and memory to the edge nodes.
- **Blackhole routing:** This technique includes rerouting all communication to a "blackhole" or a null interface, which causes all incoming traffic from the attacker to be completely ignored. Implementation of blackhole routing can take place either at the edge nodes or in the core network.
- **Rate limiting:** The pace at which incoming traffic is processed can be slowed down via rate restriction, which is a form of traffic management. This can prevent the edge nodes from becoming overrun by a surge of traffic that is being sent their way. Utilizing traffic shaping strategies or utilising hardware rate limiters are both viable options for implementing rate restriction.
- **Anomaly detection:** The process of utilising machine learning and other statistical methods to identify anomalous traffic patterns that may be an indication of a distributed denial of service assault is known as anomaly detection. If an anomaly is detected, countermeasures like traffic filtering and rate limitation can be used to address the issue.
- **Hybrid solutions:** When it comes to edge computing, a strong defence against DDoS assaults may be achieved by employing a mix of the strategies described above. For instance, malicious traffic can be prevented from overloading the edge

nodes by combining traffic filtering and rate limiting into a single preventative measure.

It is essential to keep in mind that DDoS assaults are always evolving new strategies, and it is possible that these new techniques will be able to bypass existing mitigation mechanisms. It is vital to take a preventative stance towards security, which entails doing routine monitoring and testing to ensure that the preventative measures are effective against the most recent threats.

5.2 Proposed Methods for detecting a DDOS attack and mitigations:

DDoS attacks are a form of cyberattack that aim to make networks and websites unavailable to its intended audience. The goal of a distributed denial of service (DDoS) assault is to overwhelm the target system's resources and prevent legitimate users from accessing the system by flooding the target system with traffic from several infected systems, sometimes known as "botnets." If you want to limit the damage from a DDoS assault and keep the targeted system up, you need to be able to identify when an attack is happening. The purpose of this document is to propose methods for detecting DDoS assaults.

5.2.1 Traffic Analysis:

Network security problems or attacks can be spotted with the use of a method called traffic analysis, which analyses network data for patterns and abnormalities. DDoS assaults, network breaches, and network misuse are just some of the network security vulnerabilities that may be detected by performing traffic analysis. There are several methods for performing traffic analysis, including packet capture, protocol analysis, and flow analysis.

- **Packet Capture:** The term "packet capture" refers to the process of collecting data packets in a network using a network traffic analyzer programme like Wireshark. Packets are collected so that they may be studied for irregularities and trends. Data such as IP addresses, headers, and payloads can all be obtained from a packet capture.
- **Protocol Analysis:** The process of evaluating network traffic for certain network protocols, such as HTTP or FTP, is referred to as protocol analysis. An examination of the protocol can reveal problems that are unique to the protocol, such as breaches of the protocol or efforts to gain illegal access.
- **Flow Analysis:** Flow analysis is the process of evaluating network traffic flows, which are the series of packets that belong to a single communication session. A flow is defined as the sequence of packets. The volume of traffic, the types of traffic, the origins and destinations of the traffic, and other aspects of network activity may be determined through the use of flow analysis.

There are a variety of tools available for doing traffic analysis, ranging from simple tools for capturing packets to more sophisticated platforms for conducting network research. These technologies give network administrators and security experts the ability to gather, analyse, and visually inspect network traffic in order to spot patterns and anomalies in the data that could point to possible vulnerabilities or intrusions. The following is a list of some of the most often used tools for doing traffic analyses:

- **Wireshark:** Wireshark is a tool for capturing and analysing packet traffic that is both open-source and free to use. Users are able to record network traffic, examine packet headers and data payloads, and visualise network

flows with this tool. Wireshark is capable of supporting a broad variety of protocols and has sophisticated functionality for finding and filtering packets.

- **Tcpdump**: Tcpdump is a programme for capturing packets that is used extensively in Linux and Unix systems. It operates via the command line. Users are granted the ability to record network traffic, filter data packets according to a variety of parameters, and examine packet headers.
- **NetFlow Analyzer:** When it comes to monitoring network traffic in real time, commercial tools like NetFlow Analyzer are invaluable. Users are able to track metrics like data transfer rate, network consumption, and app utilisation. The NetFlow Analyzer's superior filtering and searching capabilities, as well as its ability to issue notifications when traffic patterns differ from the usual, make it an invaluable tool.
- **Snort:** Snort is a free and open source IDS/IPS that analyses captured network traffic for signs of intrusion. Through the usage of a rule-based approach, it is able to recognise common attack vectors and issue warnings in the event of unusual network activity.
- **Splunk**: Splunk may be used for traffic analysis, as it is a commercial log analysis platform. Users are able to gather information about network traffic from a wide variety of sources, such as packet capture and flow collectors, and then evaluate that data. Splunk has sophisticated visualisation tools and may trigger notifications in response to certain network events.
- **NetWitness:** NetWitness is a commercially available technology for network research that displays data in real time. It has sophisticated tools for locating network risks and capturing and analysing network packets, flows, and log data. A complete security solution may be achieved by combining

NetWitness with other security technologies, such as those that can provide warnings based on specific network events.

As a result, traffic analysis technologies are indispensable for keeping an eye on and protecting digital infrastructures. The tool selected will be determined by factors like as the organization's desired level of security, the size of the network, and the type of network being used. In order to secure their networks from threats, administrators and security experts must be able to analyse network traffic effectively.

To perform traffic analysis, one should follow these steps:

- **Identify the network segments to be analysed:** It is important to do traffic analysis on the portions of the network that are most likely to be attacked by malicious actors. These network segments could comprise of servers, essential applications, or even the whole network.
- **Data collection:** In order to gather information, it is necessary to monitor and record network traffic and operations. This information has to be gathered over time to provide a full picture of the dynamics of the network.
- **Data Analysing:** It is important to assess the gathered data for trends and anomalies that may point to DDOS vulnerabilities or attempts at intrusion. Packet capture, protocol analysis, and flow analysis are just a few examples of the methods that may be used to analyse the data.
- **Generating alerts:** Once security threats or vulnerabilities have been discovered, notifications should be created to warn either human security employees or automated security systems. The warnings should provide specifics regarding the security problem or assault, such as the system that was attacked, the sort of attack that was carried out, and the source of the attack.

- **Respond to Alerts:** When an alert is raised, security professionals should examine the issue and take the proper action after they have determined what the problem is. Blocking traffic, isolating systems, or calling law enforcement might be among the possible actions used.

5.2.2 Real time scenario use case for DDOS detection and mitigating it using Traffic analysis:

Let's take an example of using traffic analysis tools to detect a potential DDOS attack on a company's network that is providing services to IoT devices in an edge environment. In an edge computing environment, the DDoS attack can target multiple edge devices, making it more difficult to detect and mitigate. Here's an example of how a DDoS attack can occur in an edge computing environment:

An application that is essential to the daily operations of a corporation is often hosted in a computer environment known as an edge computing environment.

Because high availability and redundancy are priorities for this application, it may be hosted on more than one edge device. After discovering the IP addresses of the edge devices that are hosting the application, the attacker starts a distributed denial of service assault by overwhelming those devices with traffic.

The assault could make use of a variety of methods, such as a UDP flood, a TCP SYN flood, or amplification of DNS traffic. In order to collect and examine the traffic that is directed to the edge devices, the network administrator makes use of traffic analysis tools such as Wireshark and tcpdump. They could see a rise in the volume of traffic or recognise patterns of traffic that are suggestive of a distributed denial of service assault.

To protect the system from further damage caused by the DDoS assault, the administrator of the network may implement any number of the following strategies.

To prevent traffic from reaching the vulnerable edge device, blackhole routing directs it to a "blackhole" or null interface instead of the targeted IP address. Through the use of access control lists (ACLs) and firewalls, harmful traffic may be filtered out through the process of traffic filtering. The filtering might be performed according to the source IP address, the port number, or the packet size.

In the process of traffic diversion, the malicious traffic is handled by the device that is being attacked, while the legal traffic is sent to other edge devices that are not currently being targeted by the attacker. The traffic and performance of the edge devices may be continually monitored by the network administrator using monitoring tools such as Nagios or Zabbix. They will then be able to notice any irregularities or departures from the typical operation of the network and take the necessary corrective action as a result.

In addition, the administrator of the network can take preventative steps. Monitoring the traffic on a network and blocking any malicious activity enables intrusion prevention systems, often known as IPS, to detect and stop distributed denial of service attacks. In rate limiting, the amount of traffic that may be delivered to a certain IP address is capped, hence preventing that address from becoming overwhelmed with an excessive quantity of data transfer requests.

5.3 DDoS attack detection model based on Bidirectional Long Short-Term Memory (BiLSTM):

The number of different types of power IoT terminal devices has grown by leaps and bounds as smart grids have been built up quickly. An attack on either of them is hard-to-protect end devices or any node in a large complicated network this can put the grid at risk. Distributed Denial of Service (DDoS) attacks create traffic that comes in short bursts. This makes it hard to use existing centralised detection methods that rely on manually setting attack characteristics to changing attack scenarios. A Bidirectional Long Short-Term Memory (BiLSTM) is a form of recurrent neural network (RNN) that is capable of processing sequential input in both forward and backward orientations.

In this, researchers propose a Bidirectional Long Short-Term Memory (BiLSTM)-based DDoS attack detection model by building an edge detection framework that is capable of extracting bidirectional contextual information about the network's environment through the use of the BiLSTM network and automatically learning the attack traffic's temporal characteristics from the original data traffic**.[12]** Combining BiLSTM with edge computing can be an effective approach for detecting and mitigating DDoS attacks. The BiLSTM can be trained to analyze network traffic and detect patterns that are characteristic of DDoS attacks. This can be done on edge devices, such as routers or firewalls, allowing for real-time detection and response.

DDoS attacks load servers and network links with enormous botnets, consuming server resources and preventing them from responding to service requests. Data shows that most DDoS attack detection solutions use servers or cloud centers. The server side must identify DDoS attacks and process requests from all parties; therefore missing network connection contexts might occur. This lets server-side DDoS attack detection algorithms parse and analyse partial network traffic packets, making DDoS attack

aberrant traffic hard to spot. To remedy the above problem, all network traffic in the same communication cycle must be forwarded to the free network segment for traffic cleaning, but this procedure would strain the already blocked network, making it unable to react to user requests in real time, which impairs user experience. Most detection approaches employ machine learning algorithms, which overemphasise feature selection and parameter training. Deep learning can categorise massive volumes of data in web applications. Deep learning has greatly improved assault detection using machine learning.

To overcome the aforementioned constraints, researchers present a DDoS attack detection approach in the power IoT based on edge computing and Bidirectional Long Short-Term Memory. The model creates a BiLSTM neural network based distributed detection technique using the idea of edge computing. In particular, edge nodes employ a DDoS attack detection paradigm to identify network services produced by IoT devices under their management.

5.3.1 Proposed Method:

Distributed Denial of Service, or DDoS, is a type of attack that hackers often use. It is easy to do and works well, and it is the hardest attack to stop.

It usually means that a zombie computer with one or more zombies is attacking a smart system by sending a large number of invalid data packets or extra business requirements. Because of the attack, the smart system doesn't work, can't be used, or is completely frozen. The general IoT architecture of any smart system is illustrated below.

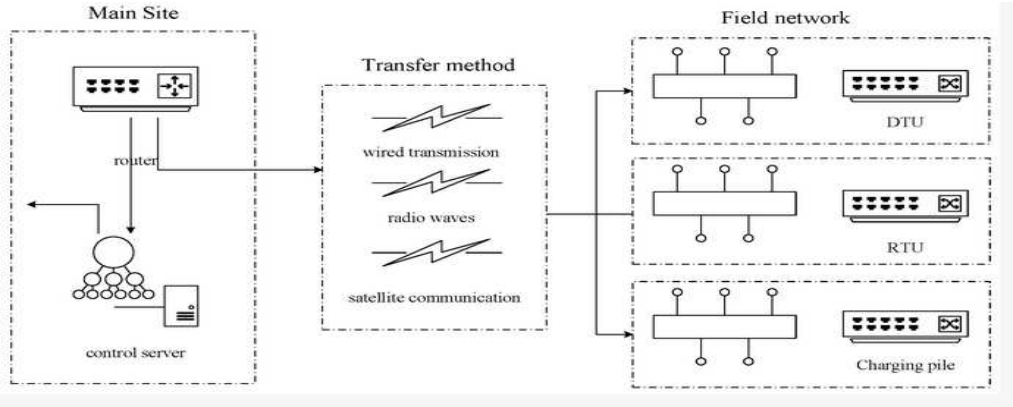

Figure 35 General Architecture of IoT system[12]

DDoS Attack Detection Framework on Edge Computing works in similar way as of any network intrusion detection systems. The suggested approach for detecting attacks on the edge of the network performs many tasks, including data collecting, data pre-processing, and attack detection. As a bonus, more modules may be added as needed to accommodate growing networks and unique traffic patterns. The following steps are followed to detect and prevent a DDOS attack.

- This data is gathered and processed by the data collection module.
- Critical service characteristics are collected by the feature extraction module and then analysed by the detection module.
- When a DDoS attack is found, a response to the attack is executed.

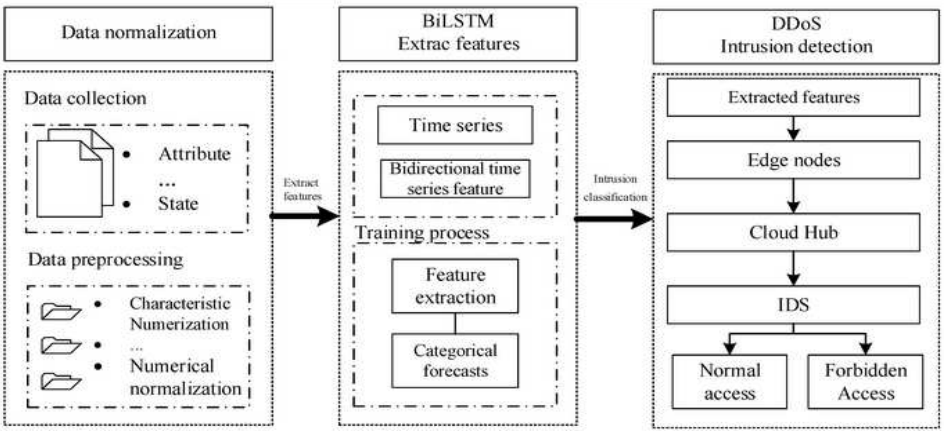

Figure 36 Overall Frame Structure[13]

As shown in the figure the BiLSTM module forms feature vectors and filters data traffic when Internet of Things terminal devices receive data streams. Edge nodes upload BiLSTM feature vectors to the cloud. The feature vector's cloud centre's history data are employed for judgement. If the retrieved feature vectors are not in the historical data, an IDS determines if their device is under attack. After flagging suspicious behaviour, traffic is immediately classified as a potential DDoS assault. The cloud centre updates the feature vectors and data, and the edge nodes get the new model. Using feature extraction and cloud updates, the BiLSTM neural network detects attacks.

Edge nodes play a crucial role in the detection of distributed denial of service attacks in the proposed architecture. The edge nodes monitor the network traffic created by the IoT devices under their care, classifying it as either normal or abnormal activity, such as that caused by a distributed denial of service (DDoS) assault. A terminal layer, an edge layer, and a cloud-computing-center layer make up the primary tiers of the network architecture.

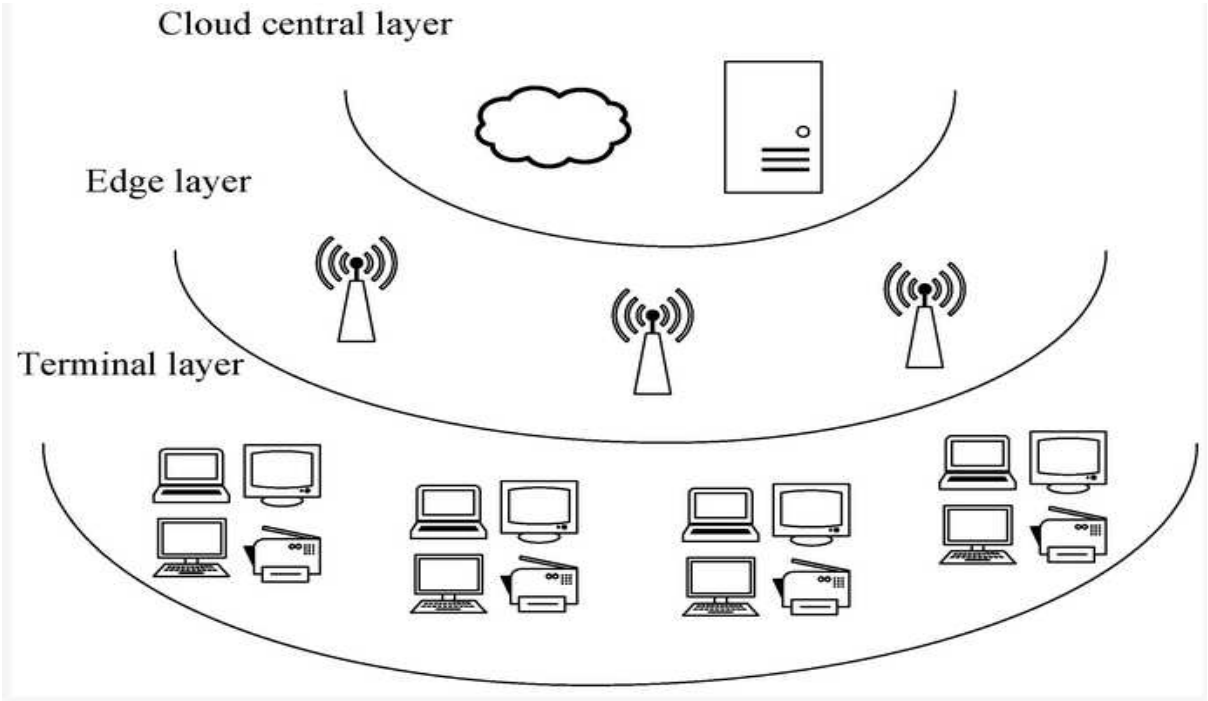

Figure 37 DDoS detection network architecture diagram based on edge computing[13]

- **Terminal Layer :** As the lowest level of the network architecture, the terminal layer is comprised of all the different types of terminal devices used to power the Internet of Things. These endpoints are frequently the source of distributed denial of service attacks.
- **Edge Layer:** The edge computing layer has several edge nodes between the terminal and the cloud centre layer. The edge part of this approach is mainly responsible for detecting DDoS attacks, collecting data about them, and storing it. The cloud centre node uploads real-time data and screens DDoS attack devices.
- **Cloud Central Layer:** The topmost layer of the detection framework is cloud-based and is responsible for training the detection model and global regulation. For efficient edge detection, the framework gathers data at the periphery, trains the model at the hub, and then pushes out the learned model to the edge nodes**.**

Bidirectional Long Short-Term Memory (BiLSTM) consists of two parallel LSTMs: one processes data in a clockwise fashion; the other is counter clockwise. At each moment, the hidden state of BiLSTM is the combination of the two states before and after, which can hide the current and future states[13]. The basic BiLSTM algorithm model trains and tests each edge node for any DDOS attacks.

5.3.1.1 BiLSTM Algorithm:

LSTM generally contains three gates at each sequence time t: forget gate, input gate, and output gate. In this paper, the current input vector x_t, the state memory unit c_{t-1} and the hidden state h_{t-1} of the previous sequence are jointly entered into the forgetting gate. The output f_t of the forget gate is obtained through a sigmoid activation function.

The calculation formula is:

$$f_t = \sigma(W_f h_{t-1} + U_f x_t + b_f) \quad (1)$$

where W_f, U_f is the weight, and b_f is the bias.

The input gate is divided into two parts: The first part uses the sigmoid activation function, and the output is i_t; the second part uses the tanh function, and the output is a_t. The two parts together determine the vector that needs to be retained in the state memory unit.

The calculation formula is:

$$i_t = \sigma(W_i h_{t-1} + U_i x_i + b_i) \quad (2)$$

$$a_t = \tanh(W_a h_{t-1} + U_a x_i + b_a) \quad (3)$$

where W_i, U_i, W_a, U_a is the weight, and b_i, b_a is the bias.

Updating the gate state, C_t consists of two parts. The first part, C_{t-1}, is the product of the output f_t of the forget gate, and the second part is the product of the output i_t and a_t of the input gate.

$$C_t = C_{t-1} \odot f_t + i_t \odot a_t \quad (4)$$

where $\odot$ is the Hadamard product.

The update of the hidden state h_t consists of two parts. The first part is o_t, which is obtained from the previous sequence of hidden states h_{t-1}, sequence data x_t, and the activation function sigmoid. The second part consists of the hidden state c_t and the tanh activation function, which is:

$$o_t = \sigma(W_o h_{t-1} + U_o x_t + b_o) \quad (5)$$

$$h_t = o_t \odot \tanh(C_t) \quad (6)$$

Figure 38 Algorithm Calculations illustration.[14]

The below figure shows how the edge nodes are getting BiLSTM training.

Algorithm 1 BiLSTM Training

Input: D : query sample set $x \subset \Re^D$

Output: (y) : the predicted label

At the edge node:
- Collect Data
- Process Data
- Upload Data to the cloud central node

At the cloud central node:

Begin:
- **for** Data Processed in Training and Test Sets:
  - Extract Features(x)
  - Extract Labels(y)
- **for** Features in x
  - Encode Features
- **for** i in range (0, n):
  - Load BiLSTM Model
  - Fit model
  - Validate model
- Test model on test sets
- The trained model is sent to the edge node

Return model

Figure 39 BiLSTM Algorithm.[15]

The processing of its attack detection method is shown in the below flow chart

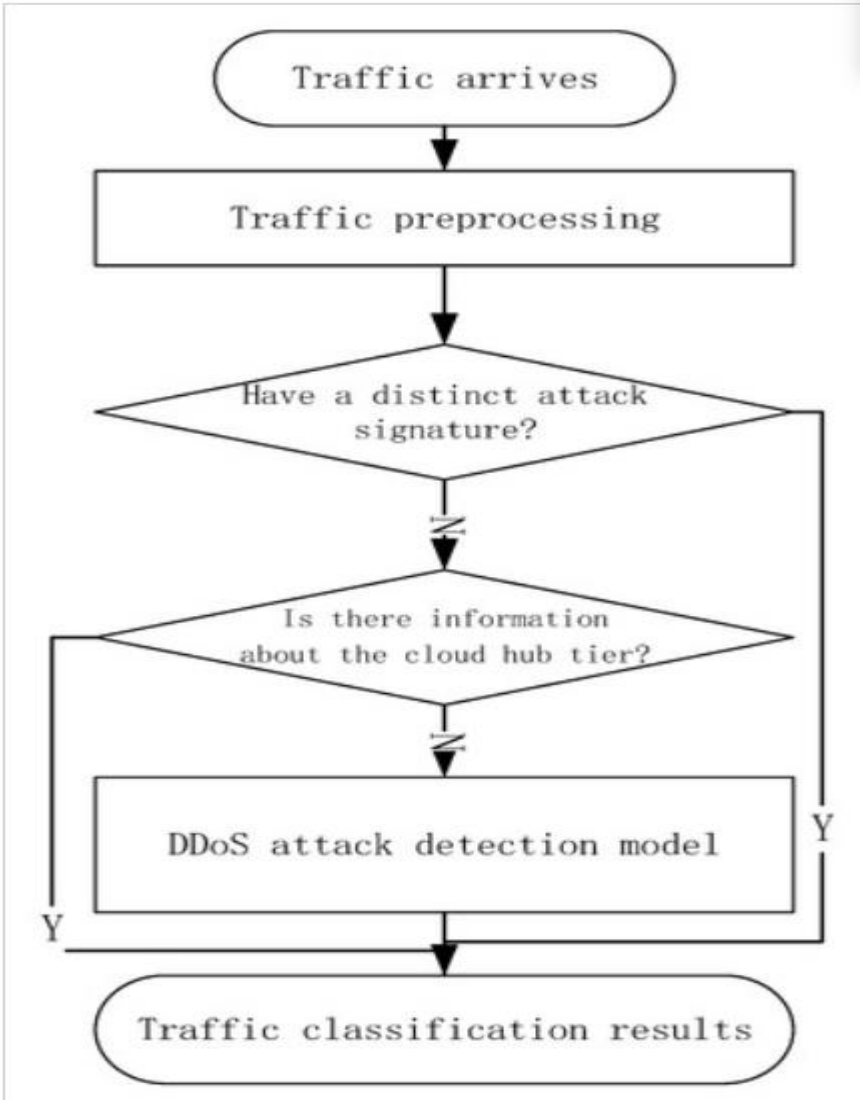

Figure 40 Flowchart of attack detection method.[15]

When compared to more advanced methods, it is clear that the suggested BiLSTM algorithm, when paired with edge computing, yields a detection rate that is more accurate when it comes to the identification of DDoS attacks. It is noted, however, that the new technique has more complexity, needs more training time, and provides the model to each edge node than do typical RNN models and LSTM models. Although the leakage rate is very minimal, it still leads in significant increases in the overhead expenses associated with communication. These restrictions are going to be improved upon in the near future.

5.4 Rogue Edge devices Use case:

In edge computing, an edge device is a device that performs data processing, storage, and communication at the edge of the network, closer to the data source or end user. A rogue edge device is an unauthorized or compromised device that is connected to the network and can potentially pose a security threat.

One real-time scenario where a rogue edge device can cause problems is in a smart city deployment. In a smart city, various devices and sensors are deployed across the city to collect and process data in real-time, such as traffic flow, air quality, and parking availability.

A rogue edge device in this scenario could be a compromised sensor that is collecting and transmitting false or misleading data to the central control system, which could cause the system to make incorrect decisions or take inappropriate actions. For example, if the traffic flow data is being manipulated, the system may suggest alternate routes that are not necessary, leading to congestion in other areas of the city.

In addition, a rogue edge device could potentially be used as an entry point for cyber attacks, as it may not have the proper security controls or protocols in place. This could compromise the entire smart city deployment, leading to serious consequences such as traffic accidents, system failures, or even human injuries.

Therefore, it is essential to ensure that all edge devices are properly authorized, monitored, and secured in a smart city deployment to prevent rogue devices from causing harm. This can be achieved through regular monitoring and updates of the devices, as well as using security protocols such as encryption and access controls to prevent unauthorized access.

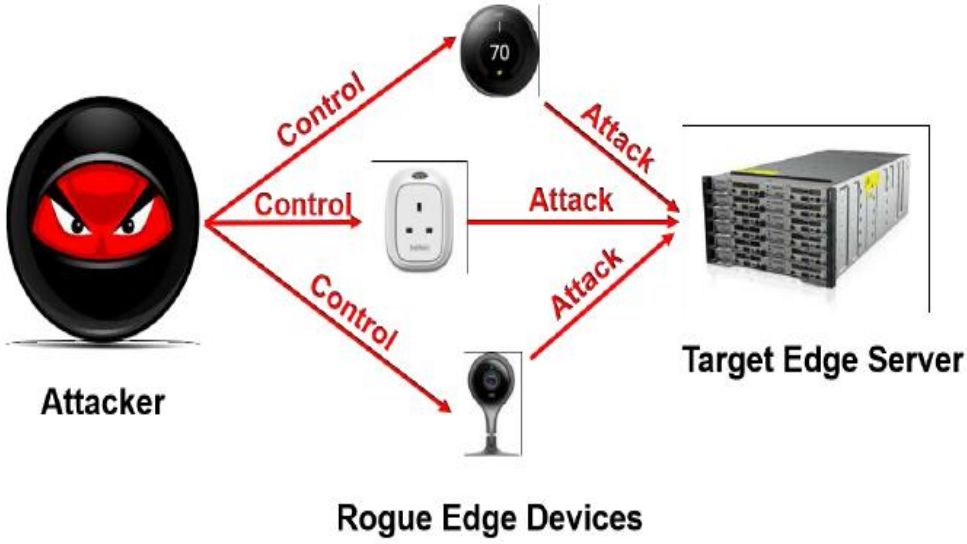

Figure 41 Typical architecture of Rogue Edge devices attack[16]

6 Conclusion:

To summarise, the expanding usage of edge computing in today 's technology has resulted in the emergence of new cybersecurity concerns, each of which calls for the development of novel solutions. The research on cybersecurity assaults and solutions in edge computing demonstrates that the security concerns in this industry are complicated and diverse. These security threats include unauthorised access, data interception, malware attacks, and device manipulation, amongst others. Moreover, it is clear that a variety of solutions, such as the use of modern encryption algorithms, secure communication protocols, intrusion detection systems, and other security measures, can be used to reduce the likelihood of these hazards. In addition, the installation of a defense-in-depth strategy, which involves a combination of technological and administrative controls, may considerably increase the security posture of edge computing systems.

It is necessary to maintain vigilance and a proactive stance in the battle against cyber threats, particularly in light of the continued rise in popularity and significance of edge computing. In order to effectively protect edge computing devices, data, and networks, a coordinated effort involving industry specialists, researchers, and regulators is required. This will allow for the development of effective cybersecurity methods and best practises. If we accomplish this, we will be able to guarantee the relentless expansion and continuous success of edge computing while also preserving the greatest possible degree of security and protection against cyberattacks.

7 References:

[1] Opeoluwa Tosin Eluwole, "“From 1G to 5G, What Next?,”," *IAENG International Journal of Computer Science,* 2018.

[2] BrainKart, "Cellular Operation," [Online]. Available: https://www.brainkart.com/article/Cellular-Operation_9920/.

[3] R. Gupta, "A Comparative Study of Various Generations in Mobile Technology," in *IJETT*, 2015.

[4] C. S. Dr. Bilel Jamoussi, "IMT-2020".

[5] ETSI, "System Architecture for the 5G System," *3GPP TS 23.501 Version 15.2. 0 Release 15.*

[6] Verizon, "Our Take on 5G and Multi-Access Edge Computing," [Online]. Available: https://www.wesleyclover.com/blog/our-take-on-5g-and-multi-access-edge-computing/.

[7] R. &. K. R. Uttarkar, "Internet of things: architecture and security.," *International Journal of Computer Application,* 2014.

[8] A. G. M. M. M. A. M. &. A. M. Al-Fuqaha, "Internet of things: A survey on enabling technologies, protocols, and applications.," *IEEE communications surveys & tutorials,* 2015.

[9] M. F. L. A. S. a. J. T. Hogan, "Nist cloud computing standards roadmap," *NIST Special Publication,* 2011.

[10] Sam Solutions, "four-best-cloud-deployment-models," [Online]. Available: https://www.sam-solutions.com/blog/four-best-cloud-deployment-models-you-need-to-know/.

[11] M. K. T. a. N. D. De Donno, "Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog," *Ieee Access,* 2019.

[12] NTT DOCOMO, INC., "WHITE PAPER 5G evolution and 6G," vol. Version 4.0, January2022.

[13] D. A. U. K. D. I. M. Q. Qazi Kamal Ud Din Arshad, "A Review on the Evolution of Cellular Technologies," in *IBCAST*, 2019.

[14] ETSI, "Why do we need 5G?," ETSI, [Online]. Available: https://www.etsi.org/technologies/5g?highlight=WyI1ZyJd.

[15] VIAVISOLUTIONS, "5G Architecture," [Online]. Available: https://www.viavisolutions.com/en-us/5g-architecture.

[16] TechTarget, "5G NSA vs. SA: How does each deployment mode differ?," [Online]. Available: https://www.techtarget.com/searchnetworking/feature/5G-NSA-vs-SA-How-does-each-deployment-mode-differ.

[17] RedHat, "what-is-multi-access-edge-computing," [Online]. Available: https://www.redhat.com/en/topics/edge-computing/what-is-multi-access-edge-computing.

[18] B. &. Madisetti, Internet of Things A hands on approach, http://www.internet-of-things-book.com, 2015.

[19] Carsten Gregersen (Nabto), "A Complete Guide to IoT Protocols & Standards In 2022," [Online]. Available: https://www.nabto.com/guide-iot-protocols-standards/.

[20] V. C. V. S. V. J. D. G. P. &. S. B. Hassija, "A survey on IoT security: application areas, security threats, and solution architectures," in *IEEE Access, 7, 82721-82743.*, 2019.

[21] P. M. S. S. Habibi, "Fog computing: a comprehensive architectural survey," in *IEEE ACCESS*, 2020.

[22] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[23] SAP INc., "what-is-cloud-computing," [Online]. Available: https://www.sap.com/insights/what-is-cloud-computing.html.

[24] A. F. C. N. T. K. K. J. F. N. A. K. J. a. J. J. Yousefpour, "All one needs to know about fog computing and related edge computing paradigms.," *Journal of Systems Architecture.*.

[25] F. J. T. J. M. R. B. J. M. L. B. a. D. L. Liu, "NIST cloud computing reference architecture," *NIST special publication.*

[26] T.-S. Chou, "Security threats on cloud computing vulnerabilities," *International Journal of Computer Science & Information Technology ,* 2019.

[27] B. W. N. B. S. K. P. &. N. D. S. Varghese, "Challenges and opportunities in edge computing," *2016 IEEE international conference on smart cloud (SmartCloud),* 2016.

[28] Altexsoft, "Edge Computing Architecture," Altexsoft, [Online]. Available: https://www.altexsoft.com/blog/edge-computing/.

[29] Y. L. Y. G. X. L. Z. Z. X. &. L. K. Zhang, "A BiLSTM-Based DDoS Attack Detection Method for Edge Computing," *Energies 2022, 15(21), 7882,* 2022.

[30] JAVATPOINT, "edge-computing-vs-cloud-computing," [Online]. Available: https://www.javatpoint.com/.

[31] Y. J. C. L. X. C. F. Y. Yinhao Xiao, "Edge Computing Security: State-of-The-Art and Challenges," *Proceedings Of IEEE,* 2019.

[32] P. Sharma, "Evolution Of Mobile Wireless Communication; Networks-1g To 5g,"," *International Journal Of Computer Science And Mobile Computing,* 2013.

[33] A. a. R. K. J. Gupta, "A Survey Of 5g Network Architecture And Emerging Technologies,," *IEEE Access,* vol. 3, no. 1206-1232, 2015.

[34] G. L. W. D. D. P. M. A. B. G. &. L. Holtrup, "5G System Security Analysis," *XIV Preprint.*

[35] A. C. H. L. Y. Y. S. L. K. G. B. M. S. &. D. L. Checko, "Cloud RAN for Mobile Networks—A Technology Overview," *IEEE,* 2014.

[36] P. a. T. G. Mell, "The nist definition of cloud computing," 2011.

[37] A. C. F. T. N. K. K. F. J. A. N. J. K. a. J. P. J. Yousefpour, "All one needs to know about fog computing and related edge computing paradigms: A complete survey."," *Journal of Systems Architecture, 98, 289-330.,* 2019.

[38] R. J. B. a. A. M. G. Buyya, "Cloud computing: Principles and Paradigms," 2010.

[39] S. A. a. M. I. Ahson, "Cloud computing and software services: theory and techniques," *CRC Press.,* 2010.

[40] F. T. J. M. J. B. R. M. J. B. L. &. L. Liu, "NIST cloud computing reference architecture," *NIST special publication,* 2011.

[41] S. a. V. K. Subashini, "A survey on security issues in service delivery models of cloud computing.," *Journal of network and computer applications,* 2011.

[42] J. Y. C. W.-S. K. a. P. L. ". o. i. v. a. a. n.-r. p. f. c. d. s. p. I. 2. 3. I. C. o. P. P. W. p. 2.-2. I. 2. Feng, "Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms.," *International Conference on Parallel Processing Workshops,* 2010.

[43] K. K. M. K. L. &. T. B. Hamlen, "Security issues in cloud computing," *International Journal of Information Security and Privacy (IJISP),* 2010.

[44] Z. a. Y. X. Xiao, "Security and privacy in cloud computing.," *IEEE communications surveys & tutorials.*

[45] A. D. D. W. P. V. &. P. A. Botta, "Integration of cloud computing and internet of things: a survey.," *Future generation computer systems,* 2016.

[46] W. J. C. Q. Z. Y. L. a. L. X. Shi, "Edge computing: Vision and challenges," *IEEE internet of things journal ,* 2016.

[47] P. A. M. D. E. A. D. T. H. A. I. M. B. P. F. a. E. R. Garcia Lopez, "Edge-centric computing: Vision and challenges.," *ACM SIGCOMM Computer Communication Review ,* 2015.

[48] B. W. N. B. S. K. P. &. N. D. S. Varghese, "Challenges and opportunities in edge computing.," *IEEE international conference on smart cloud (SmartCloud) ,* 2016.

[49] C. N. D. Y. S. G. R. H. M. M. J. &. P. P. A. Mouradian, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE communications surveys & tutorials,* 2017.

[50] M. T. W. M. F. S. &. S. S. Beck, "Mobile edge computing: A taxonomy.," *In Proc. of the Sixth International Conference on Advances in Future Internet,* 2014.

[51] G. I. Klas, "Fog computing and mobile edge cloud gain momentum open fog consortium," *etsi mec and cloudlets,* 2015.

[52] P. M. P. J. R. J. S. R. M. L. L. a. F. S. Silva, "Using edge-clouds to reduce load on traditional wifi infrastructures and improve quality of experience," *IEEE 1st International Conference on Fog and Edge Computing (ICFEC),* 2017.

[53] R. K. G. S. G. D. J. P. P. G. L. X. Y. &. R. R. Naha, "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE access,* 2018.

[54] X. a. N. A. Sun, "Edgeiot: Mobile edge computing for the internet of things," *IEEE Communications Magazine,* 2016.

[55] S. Z. H. Q. Z. Q. Z. W. S. a. Q. L. ". Yi, "Latency-aware video analytics on edge computing platform," *Proceedings of the Second ACM/IEEE Symposium on Edge Computing,* 2017.

[56] U. K. G. J. T. R. G. a. P. N. Drolia, "Cachier: Edge-caching for recognition applications," *IEEE 37th international conference on distributed computing systems (ICDCS),* 2017.

[57] Y. B. L. Y. W. H. C. M. C. C. Y. &. L. P. Lin, "IoTtalk: A management platform for reconfigurable sensor devices," *IEEE Internet of Things Journal,* 2017.

[58] "Internet of Things Global Standards Initiative," *ITU,* 2015.

[59] P. a. J. C. Gupta, "IoT based Smart Home design using power and security management," *International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH),* 2016.

[60] J. R. E. A. A. I. G. M. &. C. S. Nurse, "Smart insiders: exploring the threat from insiders using the internet-of-things.," *International Workshop on Secure Internet of Things (SIoT),* 2015.

[61] C. a. I. S. A. (CISA), "Distributed denial of service attacks.," [Online]. Available: https://www.cisa.gov/distributed-denial-service-attacks.

[62] Cisco, "Edge computing," [Online]. Available: https://www.cisco.com/c/en/us/solutions/enterprise-networks/edge-computing.html.

[63] SANS Institute, "The 2020 SANS ransomware survey: Results and analysis," 2020. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/2020-sans-ransomware-survey-results-analysis-39865.

[64] P. W. Q. H. L. &. W. H. Jiang, "Security and privacy in edge computing: A survey," *Journal of Network and Computer Applications,* 2021.

8 Glossary:

1. FDMA: Frequency division multiple access (FDMA) is the simplest way to make channels. It does this by assigning users to frequency bands that don't overlap.
2. TDMA: Time-division multiple access is a way to access channels in networks that use a shared medium. By splitting the signal into different time slots, it lets multiple users share the same frequency channel.
3. CDMA: Code-division multiple access is a way to get to a channel that is used by many types of radio communication. Multiple access is shown by CDMA, in which several transmitters can send information at the same time over a single communication channel.
4. NMT: NMT stands for "Nordic Mobile Telephone." It is a network of analogue cell phones that was built by the Nordic countries together.
5. Advance Mobile Phone System (AMPS): Advanced Mobile Phone System is a standard for analogue mobile phone systems that was first made by Bell Labs and then changed with the help of Bell Labs and Motorola.
6. RANs: Wireless communication for devices is provided by the Radio Access Network (RAN) through 5G radio FDD frequencies, allowing for the delivery of amazing new applications.
7. Millimeter wave - a high-frequency spectrum that enables faster data transfer rates but has a shorter range and can be blocked by obstacles.
8. Small cells - compact radio access nodes that are used to improve coverage and capacity in areas with high user density.
9. Massive MIMO - a technology that uses multiple antennas to transmit and receive data, increasing network capacity and improving performance.

10. Latency - the delay between a data request and its response, which is reduced in 5G networks compared to previous generations.
11. Network slicing - the ability to create multiple virtual networks with different characteristics to support diverse use cases and applications.
12. Internet of Things (IoT) - a network of connected devices that can communicate and exchange data, which is enabled by the increased capacity and speed of 5G networks.
13. Sensor - a device that detects and responds to physical or environmental changes, such as temperature, pressure, or motion.
14. Actuator - a device that converts electrical signals into physical action, such as turning a motor or opening a valve.
15. Machine-to-Machine (M2M) - communication between devices or machines without human intervention.
16. Side-channel attacks (SCA) - an attack where an attacker gains access to sensitive information by monitoring the physical signals or power consumption of an IoT device.
17. Eavesdropping and interference - an attack where an attacker intercepts or disrupts the wireless signals used by IoT devices.
18. Heterogeneity: Refers to the diversity of components used in IoT devices, which may have different hardware, software, operating systems, and applications.
19. Real-time localization: A technology that enables the tracking and monitoring of objects in real-time.
20. WPAN: Wireless Personal Area Network, a type of network that enables communication between devices over short distances.
21. Cloud computing - the delivery of computing services over the internet, including storage, processing power, and software.

22. Public cloud - a cloud computing environment in which services are delivered over the public internet.
23. Private cloud - a cloud computing environment in which services are delivered over a private network.
24. Hybrid cloud - a cloud computing environment that combines public and private cloud services.
25. Infrastructure as a Service (IaaS) - a cloud computing model in which the provider offers infrastructure components such as virtual machines, storage, and networking.
26. Platform as a Service (PaaS) - a cloud computing model in which the provider offers a platform for developing, deploying, and managing applications.
27. Software as a Service (SaaS) - a cloud computing model in which the provider offers access to software applications over the internet.
28. Virtual machine - a software emulation of a physical computer that can run multiple operating systems and applications.
29. Elasticity - the ability of a cloud computing environment to scale resources up or down to meet changing demand.
30. Containerization - a method of deploying and running applications in a lightweight, portable container that can run on any platform or cloud environment.
31. DevOps - a set of practices that combines software development (Dev) and IT operations (Ops) to improve the speed and quality of software delivery.
32. Serverless computing - a cloud computing model in which the provider manages the infrastructure and automatically scales resources to meet demand, allowing developers to focus on writing code.

33. Edge computing - a distributed computing model that brings computation and data storage closer to the location where it is needed, reducing latency and improving performance.
34. Edge devices - IoT devices or other computing devices located at the edge of the network, such as sensors, cameras, and mobile devices.
35. Edge gateway - a device that serves as a bridge between edge devices and the cloud, providing local data processing and connectivity to the internet.
36. Fog computing - a variant of edge computing that distributes data processing and storage tasks across multiple edge devices.
37. Latency - the delay between the time data is generated and the time it is processed or analyzed.
38. Bandwidth - the amount of data that can be transmitted over a network in a given amount of time.
39. Real-time processing - the ability to process and respond to data in real-time or near-real-time.
40. Artificial intelligence (AI) - the ability of machines to perform tasks that would normally require human intelligence, such as recognizing patterns or making decisions.
41. Blockchain - a digital ledger technology that allows secure, decentralized data storage and transaction processing.
42. Cybersecurity - the practice of protecting systems, networks, and devices from digital attacks, theft, and damage.
43. Threat intelligence - information about potential cybersecurity threats, including the tactics, techniques, and procedures used by attackers.

44. Intrusion detection - the process of identifying and responding to unauthorized access or activity on a network or device.
45. Authentication - the process of verifying the identity of a user or device, typically through passwords or other credentials.
46. Encryption - the process of converting data into a form that is unreadable without a key or password, to prevent unauthorized access.
47. Firewall - a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules.
48. Virtual Private Network (VPN) - a secure, encrypted connection between two devices or networks over the internet.
49. Secure boot - a process that ensures that only trusted software is loaded during the boot-up process, to prevent malware from running.
50. Trusted Platform Module (TPM) - a hardware component that provides secure storage and processing of cryptographic keys and other security data.
51. Zero trust - a security model that assumes all network traffic and devices are untrusted, and requires strict authentication and authorization for access.
52. Penetration testing - the process of simulating an attack on a system or network to identify vulnerabilities and weaknesses.
53. Incident response - the process of responding to and mitigating the impact of a cybersecurity incident, such as a data breach or cyber-attack.
54. CRM: CRM stands for Customer Relationship Management. It refers to a set of practices, technologies, and strategies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle